LogMeIn RemotelyAnywhere User Guide

April 2007

What is RemotelyAnywhere?

RemotelyAnywhere allows secure remote access to and administration of any machine on which it is installed. No special client software is required on your local machine and it is closely integrated with Windows NT/2000/XP security.

Minimize Downtime

RemotelyAnywhere helps system administrators keep IT systems up and computer users happy by offering the industry's richest remote-support toolkit. Support staff can often detect, diagnose, and solve problems faster than local support using built-in operating system functions. Background access means the user need not be interrupted during the implementation of solutions.

Deliver the Solution, Not the Person

All RemotelyAnywhere's features can be accessed securely and from any Web browser. Support and diagnostics can even be delivered from a PDA or WAP-phone browser. This means you can now offer genuine global support from anywhere, anytime.

Stop Fighting Fires

RemotelyAnywhere brings predictability to system management. By giving you monitoring, scripting, and alerts, RemotelyAnywhere allows you to detect potential problems on all your systems before they bring a halt to business. This ensures that you are often the first to know about workstation issues, ranging from attempted security breaches to unstable software installations.

Fast, Simple, Secure Enterprise Deployment

RemotelyAnywhere was designed for professionals responsible for large installations of workstations. The product is simple to install and configure on systems of anywhere between a handful and thousands of computers. Five levels of security and built-in event logging give you the confidence that your systems are safe.

Keep Your Company Productive

Less downtime means more productivity. What's more, RemotelyAnywhere can dramatically reduce IT operating costs for a surprisingly low price. Contact LogMeIn and download a free trial of our enterprise version enabling you to see these productivity gains for yourself.

Key Features

- Secure Remote Control
- Support Toolset
- Automatic Alerts
- File Transfer
- Folder Synchronization
- Remote-to-local printing
- Remote Deployment
- Accessible via Web Browser
- Enterprise Deployment
- Robust Security
- Centralized Logging
- Port Forwarding (Server Edition Only)
- Supports OpenSSH 4.5
- Supports OpenSLL 0.9.8e

Remote Control

- Complete remote control of keyboard, mouse and monitor
- Can also provide work-from-home and on-the-road access to workstations
- Dynamic resizing of desktop and adjustment of color depth
- File Transfer with delta-file updates
- Remote-to-local printing
- Automatic folder synchronization
- Compression algorithms adapts to bandwidth

Security

- Standards-compliant SSH server
- All events including unauthenticated connection attempts are logged to a central syslog server
- IP lockout of machines with a configurable number of unsuccessful logon attempts
- Security alerts and notification sent to IT managers
- Integrated Windows authentication
- RSA support

Anywhere Access

- RemotelyAnywhere can be accessed without client software
- Remote Control can be accessed using any Java or ActiveX-enabled Web Browser

- All diagnostic and administrative toolset features are presented using simple HTML interfaces
- Fully customizable interfaces support standard, light, and handheld browsers

Easy Enterprise-Wide Deployment

- Network console simplifies workstation management and remote installation
- Standard application installation
- Command line installation
- Scripted mass-deployment support
- Background installation

Support Toolset

- Background access does not interfere with computer users
- Real-time performance, connection, hardware and registry information
- Process manager with detailed info on CPU, memory, registry key and DLL usage
- Service manager with service account and dependencies
- Driver manager with dependencies
- Comprehensive user manager
- Share manager, including admin shares
- Full registry editor with ACL support
- Virtual memory settings
- Resource availability
- Emergency reboot
- Environment variables settings

Reporting and Alerts

- Catch problems before they interrupt work
- Real-time performance, resource, security, and event monitoring
- Script-defined alerts and warnings
- Powerful and flexible scripting language
- Automatic start of recovery procedures
- Alerts can be sent online, by email, or by text messages

Help Desk and Support

- Local keyboard and mouse can be disabled or kept active
- Built-in Help Desk allows interactive support for users from anywhere using your browser
- Background access allows maintenance to be performed without interrupting the user

Additional Features

- Full support for XP Fast User Switching and Terminal Services
- Custom HTTP pages can be delivered from each workstation running RemotelyAnywhere without additional of HTTP server
- Automatic check for upgrades
- User-defined colors and layouts
- User-defined quick links to the features you use most

System Requirements

RemotelyAnywhere can be used to remotely control and manage any computer running Windows Vista/XP/2000/ NT4 and Windows 98/ME.

> **Note:** Some features will not appear on Windows 98/ME machines, and this is indicated in this manual.

RemotelyAnywhere is also compatible with Windows Vista and XP 64-bit operating systems on both the local and remote machines.

Computers running RemotelyAnywhere can be accessed from most devices with ActiveX or Java-compatible web browsers, regardless of the operating system. PDA Access is limited to devices running Pocket PC 2000/2002, Microsoft Windows Mobile 2003 for Pocket PC or Microsoft Windows Mobile 2003 Second Edition for Pocket PC.

Acknowledgements

OpenSSL

RemotelyAnywhere includes cryptographic software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For more information visit: http://www.openssl.org

OpenSSH

RemotelyAnywhere uses cryptographic software developed by the OpenSSH group. For more information visit: http://www.openssh.org

CompuPhase

RemotelyAnywhere includes scripting software developed by ITB CompuPhase. The PAWN language, its interpreter and compiler are copyright © Thiadmer Riemersma, ITB CompuPhase, 1998-2007, The Netherlands. For more information visit: http://www.compuphase.com/small.htm

First Steps

About RemotelyAnywhere

RemotelyAnywhere is a remote administration tool that lets you control and administer Microsoft® Windows®-based computers over a local area network or the Internet. Originally designed for network administrators by network administrators, RemotelyAnywhere has since evolved to offer a wide variety of remote computing solutions for an equally wide variety of users. Today, RemotelyAnywhere provides such useful capabilities as Java-based desktop remote control, file transfer protocol (FTP) for downloading and uploading of files, configuration of the host computer, remote-to-local printing, advanced scripting, and dozens of other features fully detailed in the rest of this manual.

RemotelyAnywhere acts as the host software on the machine that is to be controlled or accessed. The client (the remote computer that is used to access the host) requires no special software. The client software is any Java- or ActiveX-enabled web browser, such as Internet Explorer (IE). Many RemotelyAnywhere features can also be accessed and controlled using such client software as that found in handheld PDAs.

About this Guide

This guide walks you through the process of setting up and accessing your host computer through RemotelyAnywhere.

The guide covers:

- Installing the RemotelyAnywhere software on the machine that you wish to remotely control, including:
    - Default installation configurations
    - Custom installation configurations
- Activating the software following installation.
- Accessing the host computer from a local area network (LAN) or over the Internet.
- Logging into the host machine, and the special options available.
- Bypassing the Login screen.
- Special settings required to access RemotelyAnywhere through a firewall.

Installing RemotelyAnywhere

Default Installation

1. If you have not already downloaded RemotelyAnywhere, locate and download and execute the remotelyanywhere.msi from http://www.RemotelyAnywhere.com/downloads.htm.
2. On the Welcome screen, select **Next.**
3. On the License Agreement screen, select **I Agree** if you agree to the terms and conditions. If you do not accept these terms, you can exit the setup by clicking the **Cancel** button.
4. The Software Options screen appears next. If the default listening port is acceptable, click **Next.** For more information regarding customizing RemotelyAnywhere during installation, see Custom Installation.
5. The setup will then ask for confirmation of the destination location for the files for RemotelyAnywhere.
6. If you wish to change the destination folder, select the Browse option. Select **Next** to confirm the destination folder.
7. To start copying the files to their destination folder (selected in step 6 above) click **Next.**
8. Select **Finish** to complete the Setup.

Custom Installation

1. Follow steps 1 – 4 above of the Default Installation above.
2. The Software Options screen allows the user to specify the listening port for use by RemotelyAnywhere.
3. If the default port used by RemotelyAnywhere (2000) conflicts with an existing application or service, the user may change it here. If the person installing RemotelyAnywhere is not the Network Administrator, the Network Administrator should be consulted before a port is assigned.
4. This screen also allows the user to copy configuration settings from an existing RemotelyAnywhere installation.
5. After all options have been configured satisfactorily, select **Next.**
6. Continue with steps 6 to 9 outlined above in Default Installation.

Software Activation

Once you have installed RemotelyAnywhere following the instructions above you will need to activate it. If you have already purchased a license, you will be able to paste it into the space provided and activate the software straightaway.

If you have not purchased a license but would like to do so, you will be given the option to do this on the software activation screen. If you purchase online, your license will be delivered immediately, so you can activate your software without delay. Alternatively, you may want to contact our sales department at sales@remotelyanywhere.com or by calling +1 888 246 5422 (toll free U.S.), +44 871 733 3166 (UK) or +36 1 413 3780 (international).

If you would prefer to try the software before purchasing, you are entitled to a 30-day evaluation period. Just select "I would like a free trial" on the software activation screen and follow the instructions. You will need to be connected to the Internet to activate your free trial.

The RemotelyAnywhere free trial uses an identifier value from your machine to control the number of evaluation licenses a single computer can receive. It is generated by passing unique data related to your computer through a one-way cryptographic hash function. The ID generated with this algorithm does not identify you or any component of your computer system: Think of this as a unique ticket that your machine receives.

Accessing RemotelyAnywhere

When the installation is complete, the default Internet browser will open with the address of http://MachineName:2000.

To access the host machine from a different machine, open an Internet browser and enter http://111.111.11.1:2000 on the Location/Address line. The "111.111.11.1" represents the IP address of the host machine. The "2000" represents the default port shown on the Software Options screen during installation. If you changed this port during installation, then use the specified port when accessing RemotelyAnywhere. On the same network the machine name can also be used.

On the host itself you can also access a machine by entering the loopback address http://127.0.0.1:2000 at the Location/Address line. This address allows the user to communicate with the RemotelyAnywhere installation only at the machine on which it is installed.

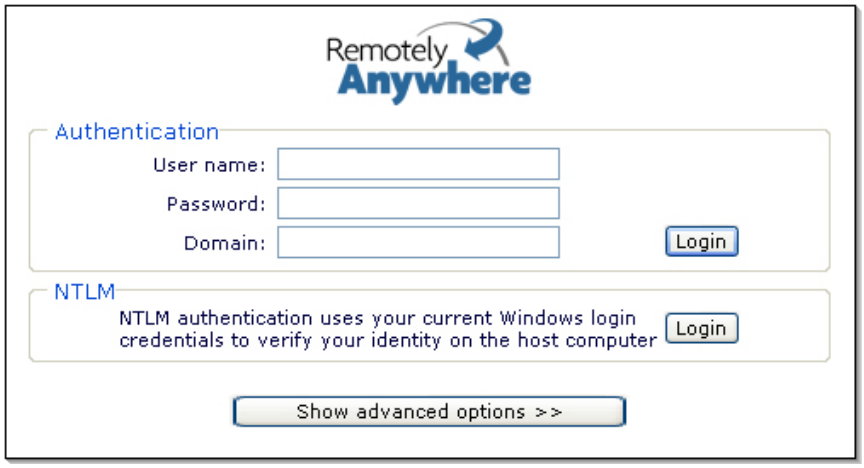
About Dynamic IP Addresses

Many DSL and cable Internet connections assign your machine a new IP address each time you connect to the Internet. This is known as a Dynamic IP address. RemotelyAnywhere will work if you have a dynamic IP (DNS) address, but RemotelyAnywhere needs to be able to track your IP address so that if it changes, the connection can be maintained. There are dynamic DNS solutions available, often for free, which means that your machine can be assigned a fully qualified and static domain name regardless of your IP address.

Alternatively, Under **Preferences > Network** you can configure RemotelyAnywhere to send you an email message pointing to the IP address of your remote host every time it detects a change. This way, you always know where to find your remote computer.

Logging In

After entering the URL into your browser and pressing enter, you will reach the RemotelyAnywhere Login screen.



RemotelyAnywhere will access the user database to authenticate the user. Initially, you will need to log on as someone who is a member of the Administrators group. You can later change this default behavior by granting NT users or groups access to RemotelyAnywhere under **Security > Access Control.**

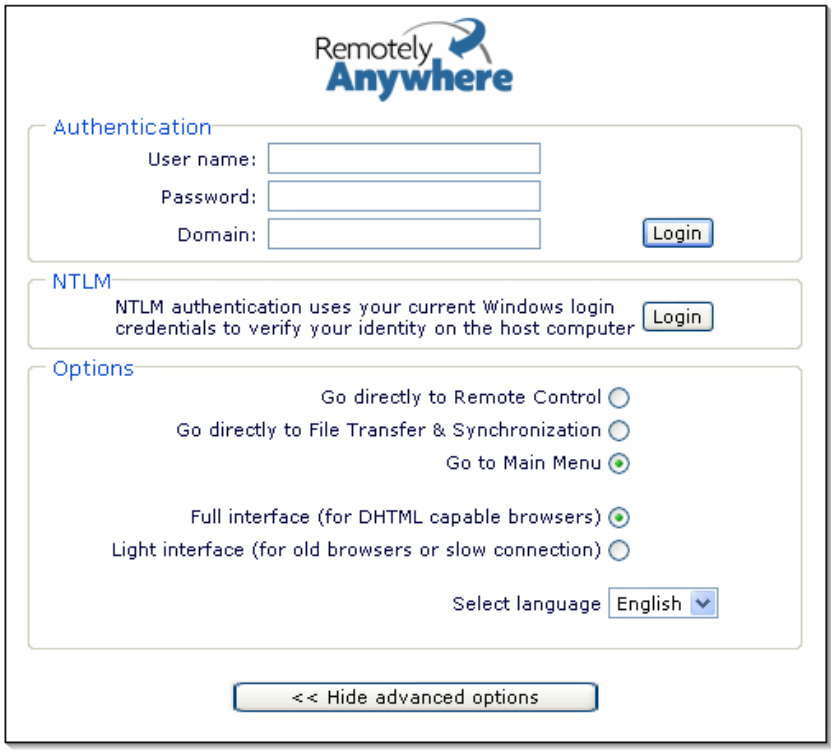
Win98 and ME users need to specify their user name during installation. If they do not, the default user name will be the machine name, and the password field will be blank.

NTLM: By clicking on the NTLM button you can use your current Windows login credentials to verify your identity on the host computer. This only works when accessing a Windows NT/2000 or XP computer. It will use your current credentials (those you entered at the NT logon prompt on the computer running your browser) to identify you to the remote computer. This is only available on local networks.

RSA Support: RemotelyAnywhere now supports RSA security. RSA SecurID offers an extra physical layer of security by demanding conclusive proof of a user's identity. If your remote machine has RSA installed, the option to use this powerful authentication method will be available on the login screen. For more information please see http://www.rsasecurity.com/products/securid/index.html.

Advanced Login Options

By clicking on **Show Advanced Options** in the login window a number of additional options become available:



Go directly to Remote Control: Using these buttons you can select whether you want to go directly into Remote Control, to File Transfer & Synchronization or to the Main Menu page - this last option being the default.

Full and Light Interfaces: You can choose between the full and light interfaces. RemotelyAnywhere's full interface is for DHTML capable browsers. The light interface is more suitable for old browsers or users with slow Internet connections.

SSL : If you set up SSL Support for RemotelyAnywhere all traffic between the host and the remote computer will be encrypted using industry-strength 128-bit ciphers, protecting your passwords and data. You can do this easily by going to Security, clicking on SSL Setup, and following the step-by-step instructions there. More information about this can be found in this manual's Section Guide.

Select Language: You are able to select the language of your choice when logging in.

Bypassing the Login Screen

You can force an NTLM login – and thus bypass the login screen entirely – by appending "/ntlm/" to the URL with which you access RemotelyAnywhere. For example, the URL http://MAILSERVER:2000 would become http://MAILSERVER:2000/ntlm/. Ensure you include the trailing slash.

You can also use this method to bypass the menu system and access certain parts of RemotelyAnywhere directly. Here are some URLs as an example:

Remote Control: http://your.machine.here:2000/ntlm/remctrl.html

Command Prompt: http://your.machine.here:2000/ntlm/telnet.html

Chat: http://your.machine.here:2000/ntlm/chat.html

Similarly, you can specify your username and password in the URL – thus forcing a normal login – by appending the credentials in a "/login:username:password:domain/" form to the URL with which you access RemotelyAnywhere. For example, the URL http://MAILSERVER:2000 would become http://MAILSERVER:2000/login:username:password:domain/. Yet again, ensure you include the trailing slash.

The Windows NT domain you are logging in to is optional. If omitted, RemotelyAnywhere will try to authenticate you on the computer on which it's running, then in the domain to which it belongs. Here are some URLs as examples:

Remote Control: http://your.machine.here:2000/login:yourloginname:yourpassword/remctrl.html

Command Prompt: http://your.machine.here:2000/login:yourloginname:yourpassword/telnet.html

Chat: http://your.machine.here:2000/login:yourloginname:yourpassword/chat.html

Accessing RemotelyAnywhere through a Firewall or Router

Most organizations today employ a range of security measures to protect their computer networks from hostile intrusion. One of the common measures includes creating a firewall. A firewall is a system designed to prevent unauthorized access to a private (internal) network. Firewalls can be implemented either as hardware or software, or a combination of the two.

The most common use of a firewall is to prevent unauthorized intrusion from Internet users attempting to access a private network or Intranet. A firewall examines all traffic entering or leaving the internal network/Intranet, ensuring that traffic meets security criteria established by the Network Administrator.

RemotelyAnywhere can be configured to work with a firewall-protected computer. This requires mapping an external, incoming port on the firewall to the internal IP and port on the computer running RemotelyAnywhere. Routers, on the other hand, operate in much the same way as firewalls. They both offer the opportunity to open

and map ports to specific computers. For the rest of this explanation, the term "router" can be interchangeable with "firewall."

From outside your LAN, you would gain access to the computer running RemotelyAnywhere by entering the firewall's IP address and the port to which the desired machine is mapped. For example:

Router: External IP address: 111.111.111.111

RemotelyAnywhere computer: IP address: 192.168.0.10, Port: 2000 (port 2000 is the default but this can also be changed).

Step 1: Mapping a Firewall Port to the Computer

In this case, you would pick a port on the router (say, 5200) and map it to 192.168.0.10:2000.

The procedure for mapping ports from routers to computers is router-specific. Usually your router will have a web-based interface that allows you to configure and maintain it. Sometimes router companies refer to this action as Port Forwarding or Port Mapping.

Step 2: Accessing RemotelyAnywhere through a Firewall

Having done the above, you will now be able to fully access the RemotelyAnywhere computer with the URL http://111.111.111.111:5200 - that is the firewall's external IP, followed by the port you mapped to the RemotelyAnywhere machine.

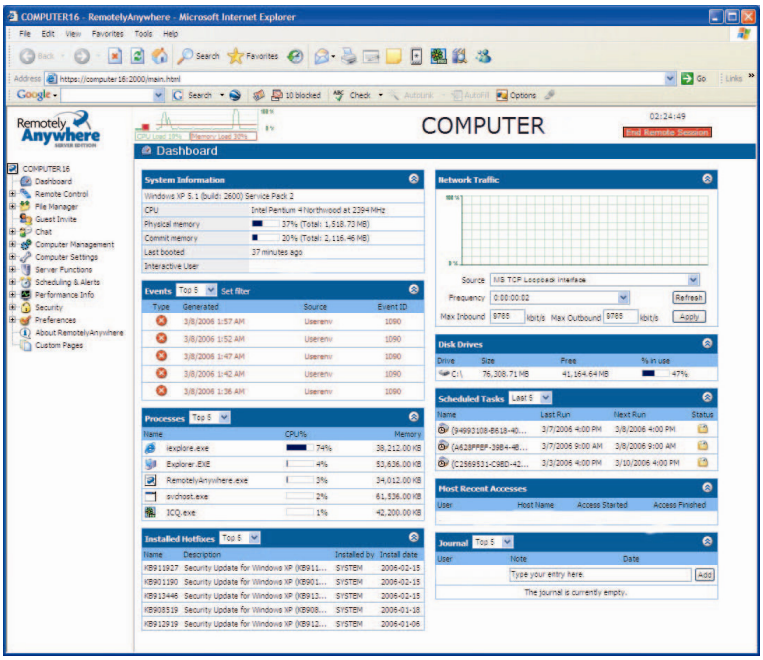
External Resources for Help with Router and Firewall Configuration

No two router models are exactly alike, and this document lacks sufficient space or scope to offer detailed support for all routers and firewalls and RemotelyAnywhere. However, the overarching principles for port forwarding remain the same. Should your router or firewall documentation prove confusing or insufficient, there are several resources available on the Internet that provide exhaustive instruction and help with configuring routers and firewalls.

User Interface

The user interface is designed to make using RemotelyAnywhere quick and easy. The best references for using RemotelyAnywhere are the Section Guides which follow this chapter. There, the functionality of every feature is detailed at length. In this chapter, however, we will outline those interface features that are consistent throughout the tool.

When you start up RemotelyAnywhere 7 this is what you see:



The Dashboard

The System Dashboard gives you a detailed, up-to-the-minute diagnostic view of the system info on your RemotelyAnywhere host. Each window on the Dashboard displays a summary of activity you can view in further detail by clicking on the window heading. The headings include System Information, Network Traffic, Events, Disk Drives, Processes, Scheduled Tasks, Most Recent Accesses, Installed Hotfixes, and the Journal.
The Dashboard is also interactive: you can drag, drop, minimize, maximize or reposition the applet windows displayed. You can even leave helpful notes on the computer's desktop with the Dashboard's Journal feature.

The Menu

Every page of RemotelyAnywhere can be reached from the left hand menu tree. The menu tree is expandable and collapsible like Windows Explorer so you can find the pages you need quickly. There are new categories for RemotelyAnywhere's extensive range of features so that the tool's functionality is now more transparent than ever before. These are shown at the top of the next page.

The sub-sections of each of the above categories are labeled as follows in the menu:

This means that the page contains data that can be modified. It is a configurable page.

This icon shows that a page just displays data. Although you may be able to refresh the page in order to get the latest data, you cannot interact with or in anyway modify what is shown from this location.

For more information about the above sections, please refer to this manual's Section Guide.

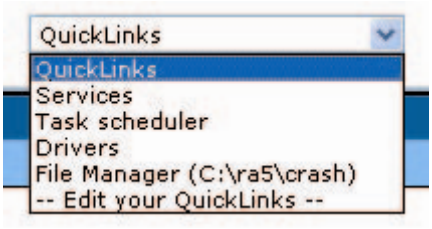
Performance Data Viewer

On every page of RemotelyAnywhere you can see a real-time Performance Data Viewer:

This java applet is to the right of the RemotelyAnywhere logo in the top frame. It shows CPU load (green) and Memory load (red) and is updated every few seconds, so you can get instant feedback on the effects of performance intensive processes.

This graph can be disabled under **Preferences > Appearance.**

Quicklinks



QuickLinks are another new feature accessible from every page of RemotelyAnywhere. You can add your favorite pages to the QuickLinks drop down menu wherever you see the star icon in the tool bar of the page you are viewing. You can also edit your QuickLinks by clicking on Edit your QuickLinks in the QuickLinks drop-down menu.

The QuickLinks menu is situated in the top frame of the page so that your favorite pages are always only a click away. They are also listed on the System Overview tab of Home page.

Log Out and Time

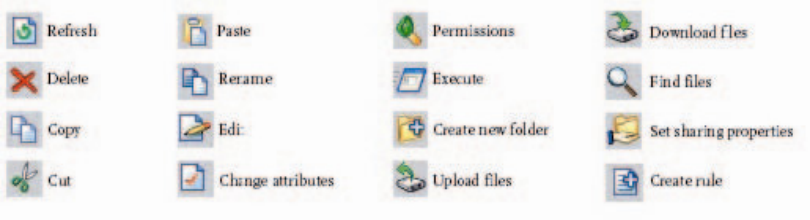
You can Log Out from RemotelyAnywhere via the red Log Out button in the top right corner of the screen, to the right of your computer's name. If you are inactive for 10 minutes you will be logged out automatically. The session timeout time can be modified under **Security > Access Control.**

The time on the remote machine is displayed above the log out button.

The Main Content Window

The main content window is where you will carry out most of your interaction with the host machine via RemotelyAnywhere. For the most part this should be self explanatory. The Remote Control window can be detached from the main pane – you will read more about this in the relevant part of the Section Guide.

On most pages you'll see a tool bar at the top. Below is a quick key to the buttons you'll encounter on these toolbars.



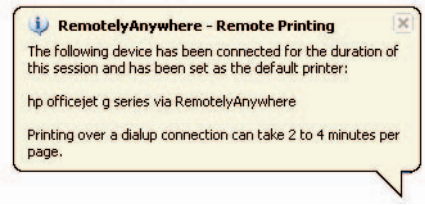
For more information about commands specific to certain pages, see Section Guide - Remote Control.

System Tray Icon

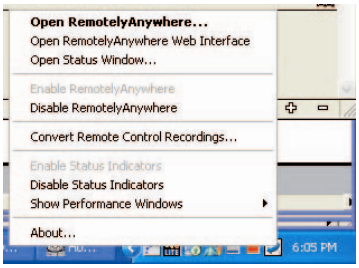
RemotelyAnywhere includes a system tray icon that serves multiple purposes. This icon can be fully configured via the **Preferences > Systray Settings** screen.

The icon will blink whenever someone is accessing the computer with RemotelyAnywhere. Double-clicking the tray icon will bring up a dialog that shows the most recent events that have occurred within RemotelyAnywhere.

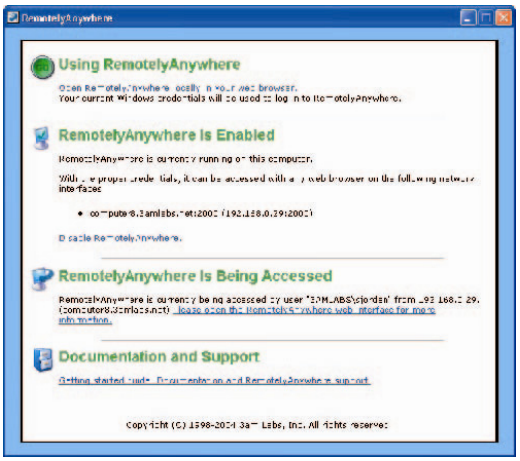
A user sitting at a Windows XP host computer will be notified of remote printing:



Right-clicking the RemotelyAnywhere icon in the systray will bring up the following menu:



Open RemotelyAnywhere: This option will open this dialog box:



Open RemotelyAnywhere Web Interface: This option will start up RemotelyAnywhere on the local host and log you in using NTLM.

Open Status Window: This option opens a window that updates you on the current status of RemotelyAnywhere.

Enable/Disable RemotelyAnywhere: Here you can turn the RemotelyAnywhere service on and off at will.

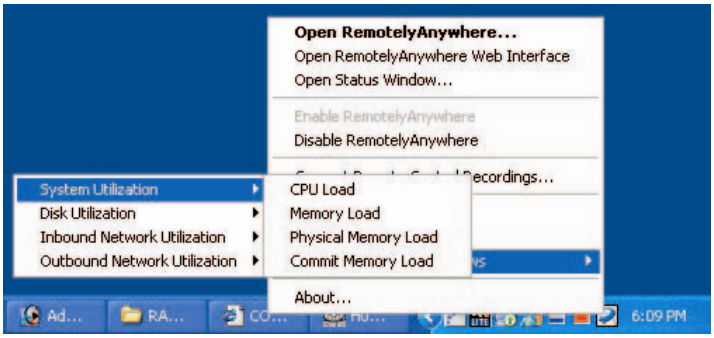
The above dialog box is displayed when you click on Open RemotelyAnywhere in the menu available from the systray icon or from your Start menu. In addition to the other context menu items (open the web interface, enable/disable RemotelyAnywhere) you can see if RemotelyAnywhere is currently being accessed, and access the documentation (including this guide). You will also be alerted via this screen if RemotelyAnywhere's license has expired or the software has not been activated.

Enable/Disable Status Indicators: Here you can enable or disable the memory and CPU usage indicators.

About: This command brings up RemotelyAnywhere's HTML About box.

Convert Remote Control Recordings: This wizard will convert RemotelyAnywhere remote control screen recording files into an AVI file for playback in any media player.

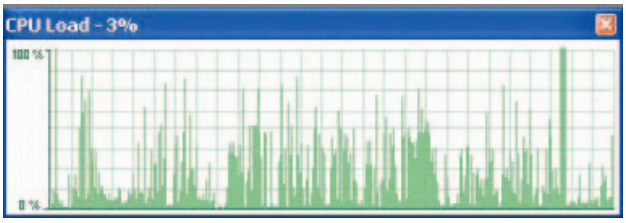
Show Performance Windows: This item will open the following submenu:



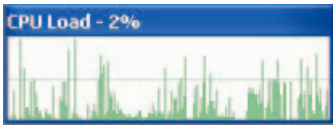
In this menu, you are given a selection of performance indicators to display on your desktop.

What actually appears in this menu is based on the performance data RemotelyAnywhere is able to collect. The software automatically collects performance data on CPU usage (total and broken down by individual CPU on SMP systems), and various memory counters.

When you select an item from this menu, a window will pop up:



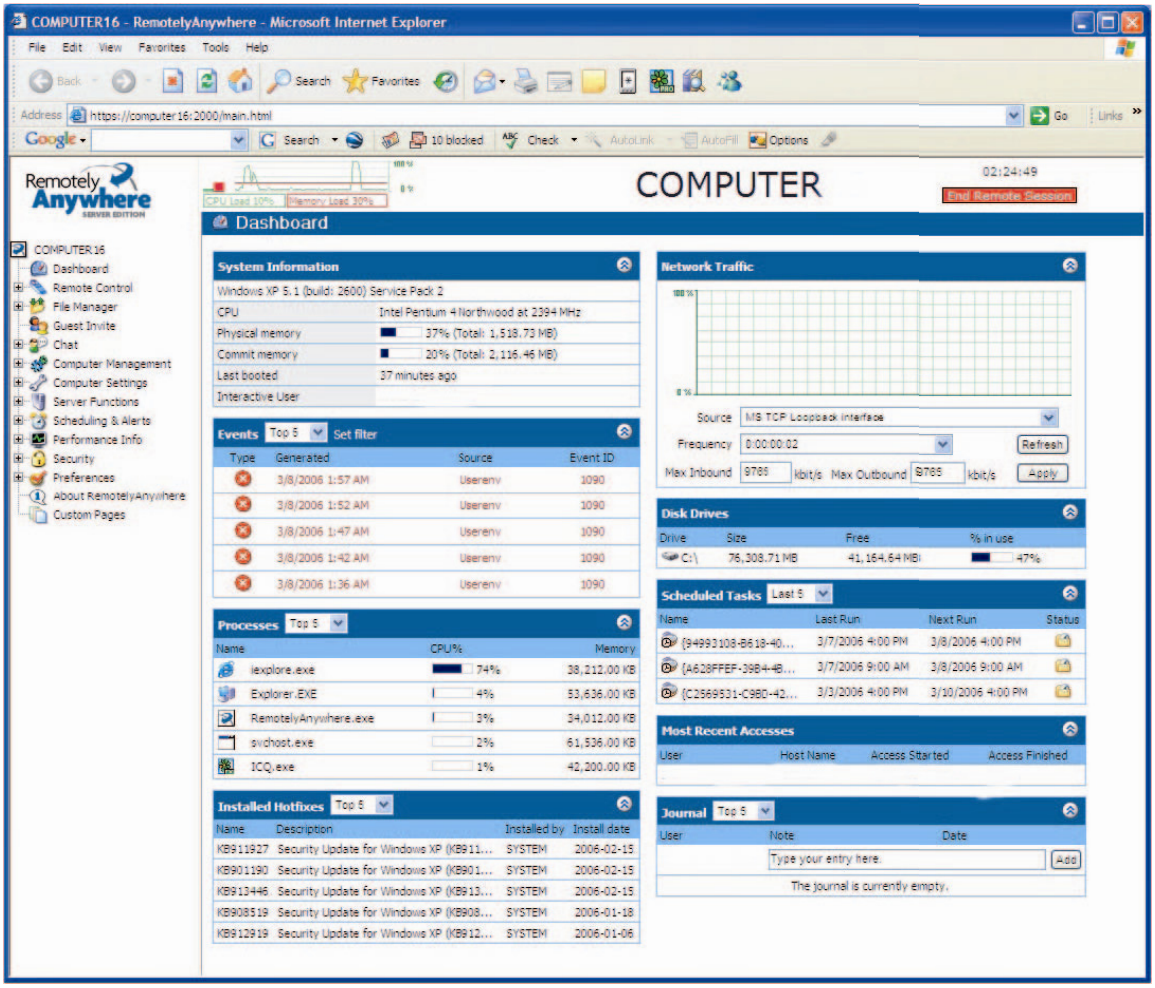
Double-clicking the performance window will shrink it to a smaller format:



You can have as many of these windows up on your screen as you want. They are persistent – that is, they will automatically appear in their previous position following a reboot.

The Dashboard

The Dashboard is the page that you'll see when you first start up RemotelyAnywhere. There you will find a useful at-a-glance System Overview and more general information about RemotelyAnywhere itself is available if you click on the About RemotelyAnywhere tab. It contains a multitude of useful information about the host computer.

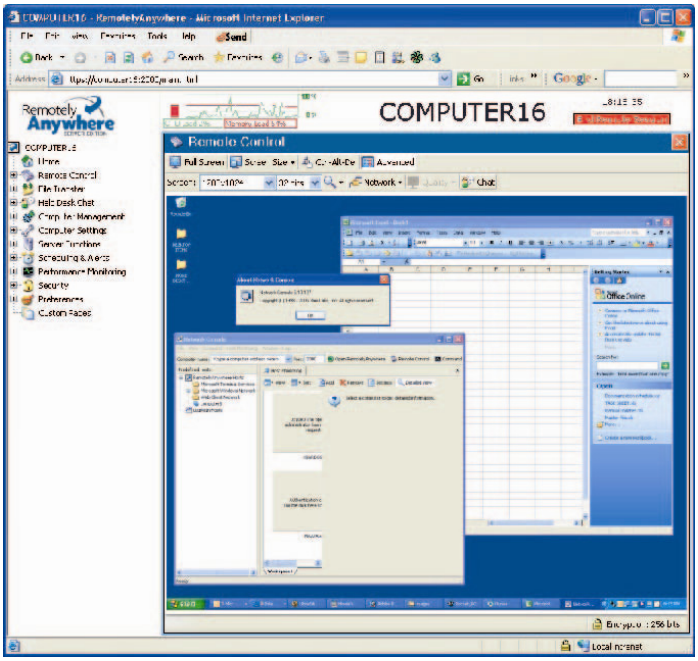


The Dashboard gives you a detailed, up-to-the-minute diagnostic view of the system info on your IT Reach computers. Each window on the Dashboard displays a summary of activity you can view in further detail by clicking on the window heading. The headings include System Information, Network Traffic, Events, Disk Drives, Processes, Scheduled Tasks, Most Recent Accesses, Installed Hotfixes and the Journal.

The Dashboard is also interactive: you can drag, drop, minimize, maximize or reposition the applet windows displayed. You can even leave helpful notes on the computer's desktop with the Dashboard's Journal feature.

Remote Control

One of the main features of RemotelyAnywhere is its advanced ability to remotely control the computer on which it is installed, thus enabling you to authentically replicate the experience of sitting in front of the host computer - regardless of where you actually are in the world.



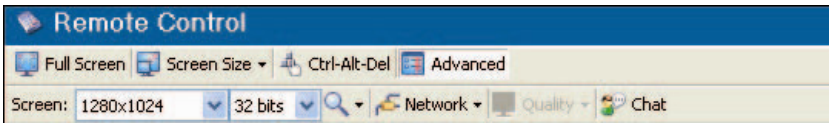
When you select Remote Control, by default RemotelyAnywhere will attempt to load a small ActiveX control, and, if your browser does not support ActiveX, it will try the Java-based version. Failing that, the HTML screenshot version will load.

By expanding the left Remote Control menu, it is possible to select any of these three options manually. Depending on your browser settings, you may see a pop-up window asking you to accept or reject the ActiveX control or Java applet. You should accept it in order to use Remote Control.

When typing or using your mouse, it will be exactly as if you were sitting in front of the remote machine. The only real difference will be a number of RemotelyAnywhere-specific tools which appear at the top of the remote control window, detailed below.

ActiveX Version

The ActiveX version of RemotelyAnywhere's remote control, which is what launches by default, offers a substantially different interface to the Java version.



Full Screen

This launches a true full screen in the remote window. Moving the pointer to the top of the screen will bring a drop-down toolbar showing the same options available in the regular remote control interface. Clicking **Full Screen** again will return the screen to the regular interface.

Screen Size

There are four options here:

1. **View Actual Size:** Renders a 100% view of the host screen.
2. **Fit to Window:** Adjusts the zoom on the host screen to make the window fit the screen.
3. **Match Resolution:** Resizes the host computer's desktop to fit the resolution of the remote screen.
4. **Zoom:** Manually adjusts the zoom ratio.

Send Ctrl-Alt-Del

Use this button to send a Ctrl-Alt-Del keystroke combination to the host machine.

Advanced

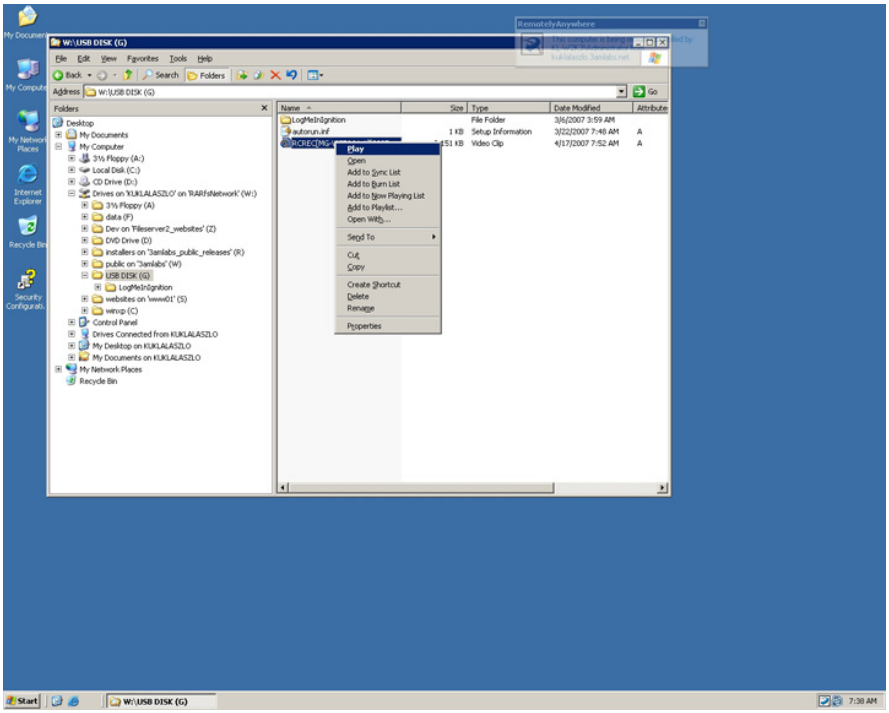
Brings up a further layer of remote control options. Click this again to hide the advanced interface.

Screen:

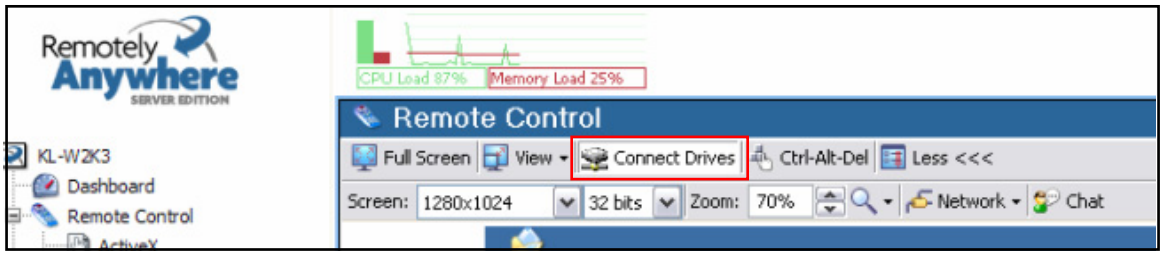
Resizes the host desktop to one of an available range of predefined resolutions.

Disk Mapping

It is possible to map drives on the host machine so that they are directly accessible from the remote machine – just as if the drive was physically on the remote machine. For example, you may have an .msi installer file on the host machine and you wish to run that .msi on the remote machine, thus avoid the need to send the file via email or FTP transfer.



To access the feature, click on the **Connect Drives** button when on the Remote Control screen and the drives on the two machines will automatically be mapped, so that files on the local machine can be accessed and run on the remote machine.



Bit Depth Drop-down menu

Depending on the capabilities of your host machine's video card, you can reset the color depth of that machine to 4, 8, 16, 24, or 32 bits. The lower the bit depth, the fewer colors and the faster the remote control performance.

Enable Magnifier

This launches a magnifying box that can be placed anywhere on the screen. This is useful for when you are remote controlling while zoomed out, but would like to examine the host screen in detail.

Network Settings

Here you can configure your link speed options. We recommend the Auto setting, but it is possible to force the link speed.

Quality

Users with slower connections will note a performance increase as the remote control quality option is adjusted downwards. However, the quality of the screen image transmitted may be degraded.

Chat

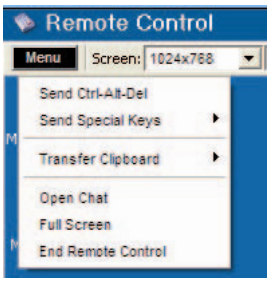
Using this feature you can chat with an interactive user of the remote host. Having clicked on the Chat button a text field opens beneath the toolbar in which you can enter and send messages. These messages will be displayed on the remote desktop, much as with RemotelyAnywhere's Help Desk Chat feature, which is documented later in this manual.

Mozilla Version

Select this option in the left-side navigation pane if you are connecting to a RemotelyAnywhere host with a client using a Mozilla web browser.

Java Version

In the top left corner of the remote control screen you will see the menu:



Remote Control Screen Grayscale Feature

To save Internet bandwidth hogging, whenever the remote control screen becomes inactive on a machine, i.e. the mouse cursor moves off the remote control window, the remote control display automatically reverts to grayscale. As soon as the cursor returns to the remote control window, the color returns to that specified in Preferences.

Send Special Keys

Some actions, such as sending Ctrl-Alt-Delete, cannot be captured by the Applet, but you can still send them via the menu. If you select **Send Special Keys** you will gain access to a whole list of special key combinations you might need to send to the host computer.

Full Screen Remote Sessions

This detaches the remote window allowing you greater flexibility. When in full screen mode you can easily switch back to the standard RemotelyAnywhere frame by selecting **Exit Full Screen.**

You can also do this with the close and maximize icons in the top right corner of the remote window.

Whiteboard

During a remote control session, you can select to use an interactive crayon to draw or highlight items on the remote computer's screen. Simply select **Whiteboard** from the Remote Control drop-down list.

Laser Pointer

During a remote control session, you can select to use an interactive laser pointer-type red dot to highlight items on the remote computer's screen. Simply select **Laser Pointer** from the Remote Control drop-down list.

Display Properties

You can also modify the remote screen's display properties via the menu. There are drop-down menus for color and screen resolution, as well as a zoom option that allows you to view the screen all the way up to 300% of its original size.

For the optimum performance during remote control, you should set the remote machine's screen resolution to the lowest, still workable value. It is also recommended that you do not use 16-bit (hi-color, 65536 colors) for the remote host's display. Use either 256 colors or true color. Converting 16-bit color bitmaps down to the internal format can be slow and have a negative impact on performance.

Remote Clipboard

Another useful option available from the menu is the ability to transfer your clipboards between machines, thus allowing you to copy from one machine and paste on the other.

For example, if you copy some text on the local machine, then select from the menu on the remote screen: **Transfer Clipboard > Local to Host.** The same applies vice-versa, but you would select **Host to Local** in order to transfer your clipboard between machines.

The limit is 8MB in both directions. If the clipboard is larger it will not do anything. On the MS JVM it only supports Unicode text. With Sun, it also works with bitmaps.

Chat

Using this feature you can chat with an interactive user of the remote host. Having selected the Chat button, a text input field opens beneath the toolbar wherein you can enter and send messages. These messages will be displayed on the remote desktop, much as with RemotelyAnywhere's Help Desk Chat feature, which is documented later in this manual.

Terminal Servers

This feature enables you to attach your remote control connection to an existing terminal server session. By default, RemotelyAnywhere reads the display output in order to show the remote desktop. Terminal server sessions are not included in this display output. In effect, they are hidden from the desktop, but RemotelyAnywhere is able to display and interact with them in a way that would not ordinarily be available to an interactive user of the host machine.

Remote Control Toolbar

In addition to the Menu options and the ability to change screen resolution and magnification on the fly, the following options are available via the remote control toolbar:

Send Ctrl+Alt+Delete: This option is found under the Menu option during browser based RemotelyAnywhere Remote Control, and you'll need this to unlock a remote machine.

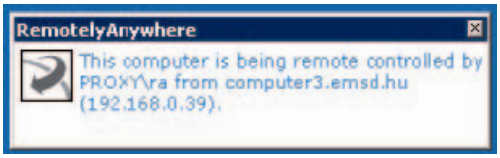
Network: Here you can configure your link speed options. We recommend the Auto setting, but it is possible to force the link speed.

Other Remote Control Features

Remote Notification

When you initiate a remote control session, a notification message will appear on the remote screen. If you do not have full administrative rights on the remote machine, a user sitting there would be invited to decline or accept the remote session. There is a default delay of 10 seconds, following which you are connected automatically. You can configure both the message displayed and the amount of time given to make a decision under **Preferences > Remote Control.**

When a remote session is in progress, a small window in the top right corner of the remote screen is displayed. This advises who is currently remotely connected to the machine. This message can also be configured under **Preferences > Remote Control.**



Remote Printing

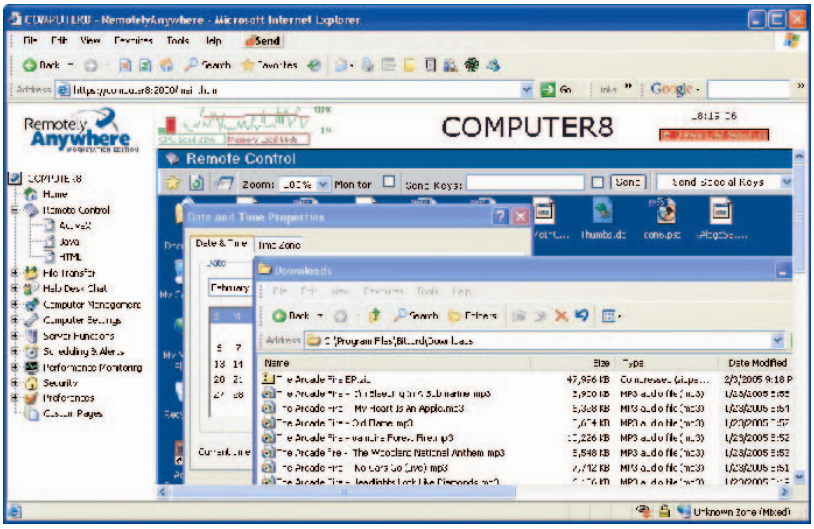
When connected to the remote machine, and if you have remote printing enabled (under **Preferences > Remote Control**) that machine's default printer will temporarily become that of your local machine. This means that should you choose to print anything from the remote machine, you will receive it on your local printer.

A user sitting at the remote machine would be notified of this change.

Remote Control Preferences

There are a number of special features you can use to configure your remote control sessions under preferences. These are detailed in the Preferences section towards the end of this chapter under **Preferences > Remote Control.**

Screenshot-based Remote Control



If the client you are using is not ActiveX or Java-enabled, or for whatever reason your connection is too slow, you might want to make use of Screenshot-based Remote Control.

In order to use this feature, you'll first need to set it as the default for Remote Control under Preferences > Remote Control. You can switch back to ActiveX or Java Remote Control any time.

If you have Screenshot-based Remote Control enabled, this is what you'll see when you click on Remote Control in the left hand menu:

The remote screen is a clickable image map, with which you can interact right on the page to some extent (clicking on buttons, right clicking) but for the most part you will have to use the toolbar at the top.

To enter text on the remote screen, you should enter it in the send keys field in the toolbar and click send. Checking the box next to this field enables you to enter special characters and simulate special keys. Each key is represented by one or more characters. To specify a single keyboard character, use the character itself. The plus sign (+), caret (^), percent sign (%), tilde (~), and braces {} have special meanings to this function. To specify one of these characters, enclose it within braces ({}). For example, to specify the plus sign, use {+}. To specify brace

characters, use {{} and {}}.

To send special key combinations such as Ctrl+Alt+Delete, use the drop down menu to the right of the send keys field.

To specify characters that are not displayed when you press a key, such as Enter or Tab, and keys that represent actions rather than characters, use the codes shown below:

Key Code	
Backspace	{BACKSPACE}, {BS}, or {BKSP}
Caps Lock	{CAPSLOCK}
Del	{DELETE} or {DEL}
Down Arrow	{DOWN}
End	{END}
Enter	{ENTER} or ~ ESC {ESC}
Home	{HOME}
Insert	{INSERT} or {INS}
Left Arrow	{LEFT}
Num Lock	{NUMLOCK}
Page Down	{PGDN}
Page Up {PGUP}	
Right Arrow	{RIGHT}
Scroll Lock	{SCROLLLOCK}
Tab	{TAB}
Up Arrow	{UP}
F1 to F24	{F1} to {F24}

To specify keys combined with any combination of the Shift, Ctrl, and Alt keys, precede the key code with one or more of the following codes:

Key Code	
Shift	+
Ctrl	^
Alt	%

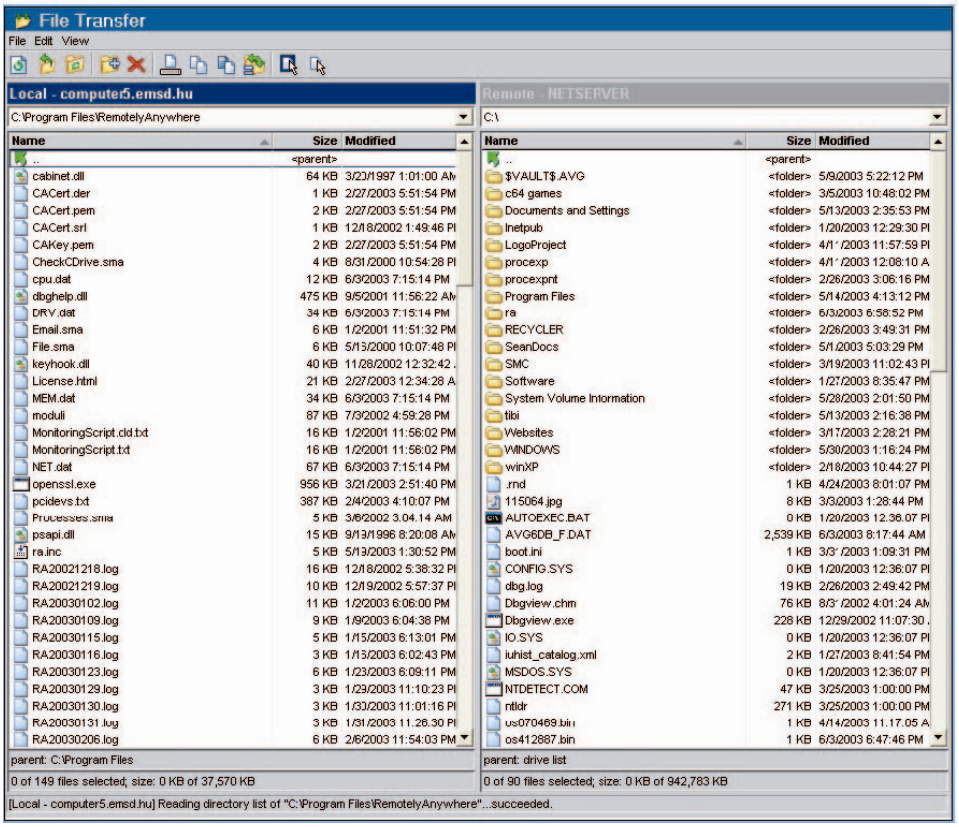
For example, if you want to go to the beginning of an edit field, select the entire line, place it on the clipboard, and overwrite it with something else then select Enter, you would type:

{HOME}+{END}^cThis is the new text {ENTER}

This translates into pressing the Home key (going to the beginning to the field), pressing the Shift and the End keys at the same time (selecting the entire field), pressing Ctrl+C (clipboard copy), typing the new text and then selecting Enter.

File Manager

With RemotelyAnywhere's ActiveX or Java-based File Transfer you can quickly and securely transfer files between the local and the remote computer. All data transferred between the two computers are compressed and encrypted.



This manual details the Java-based version of File Transfer. The ActiveX version, which defaults on Internet Explorer, functions in exactly the same way and contains only minor cosmetic differences.

As in the screenshot above, the screen is divided into two panels. The left panel shows the file tree of the computer running the web browser. The right panel displays the remote computer's file tree.

You can use the icons at the top of the screen, or your keyboard and mouse, to operate the File

Transfer Applet. There is always an active and inactive panel and you can switch easily between them with the Tab key.

Refresh: You can refresh the list by selecting the refresh button, or by pressing F5 on the keyboard.

Up: You can go up to the parent directory by clicking the **Up** button, or by pressing the Backspace key on your keyboard.

Goto Folder: To go to a different folder, click on the **Goto folder** button, or use the Ctrl+G key combination.

Create folder: You can create a new folder with the **Create folder** button or by pressing Ctrl+N.

Delete: You can delete a folder or file with the delete button, or by pressing Delete on your keyboard.

Rename: You can rename a file or folder with the Rename button or by pressing F2.

Copy: You can copy a file or folder with the copy button or by pressing Ctrl+C.

Move: You can move a file or folder with the Move button or by pressing Ctrl+X.

Synchronize current folders: By clicking on the Synchronize current folder button (or by pressing Ctrl+S), you can synchronize the folders on local and remote machines.

Replicate Current folder: This button allows you to synchronize one way from one folder to another.

Select files: You can select files with the Select files button or by pressing + on the number pad.

Deselect files: You can also deselect files via the toolbar or with the "-" key on the number pad.

Guest Invite

With RemotelyAnywhere's Guest Invite feature you can securely share your remote computer's desktop with a trusted friend or colleague for enhanced collaboration and support.

To use the feature, you must be physically present at the RemotelyAnywhere host computer your guest will access. To invite a guest to your host computer's desktop, do the following:

- Right-click on the RemotelyAnywhere system tray icon and select **Guest Invite**.
- Follow the Guest Invite Wizard instructions and, when prompted, select how long the invitation to your desktop will be valid.
- Next, enter your guest's email address and an optional text message.
- Click **Finish** and your guest will be sent an email containing a special link they can click to remotely access your desktop.
    - Note: You can also use this features by clicking Guest Invite on the navigation bar to the left of your browser window.
- Once your guest clicks the special link in the email, they will be prompted to select whether to synchronize your computer's clipboard with their own.
- Once your guest clicks Continue, you will be prompted on your local computer by the dialog box below to

grant them access to your desktop. If you do not grant access within 30 seconds, it will be refused.

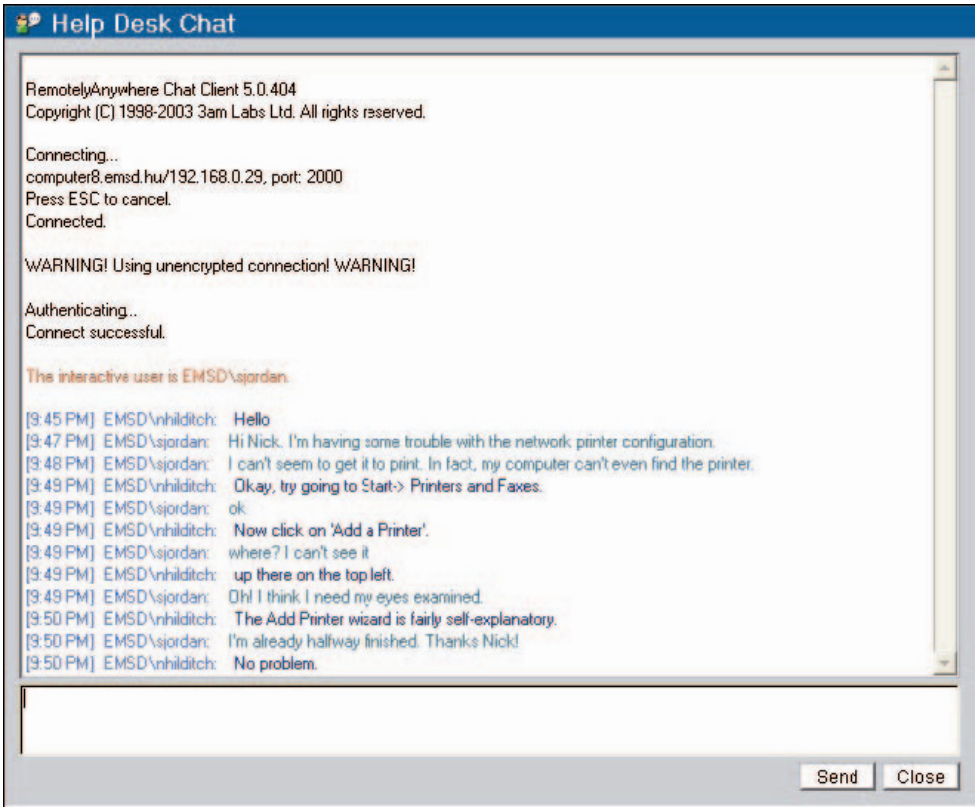
You will next be prompted to select whether to allow your guest view-only or full remote control access to your desktop.

Note: Once your guest's remote control session on your desktop begins, a dialog box will appear on the desktop. Click **Disconnect** in the dialog box at any time to end the remote control session.

You can also activate, cancel or clear any or all of the emails you send to guests you have invited to your desktop; simply right-click on the LogMeIn systray icon and click **Guest Invite > View Pending Invitations**.

Help Desk Chat

RemotelyAnywhere's Help Desk Chat feature allows you to communicate with the user sitting in front of the remote computer as you would with any instant messaging software. Thus, RemotelyAnywhere's advanced diagnostic capabilities can be put to use while you are remotely connected.



Type new messages in the lower pane and select **Send.** Earlier messages in the conversation between the two parties appear in the upper pane. Connection and session connection data also appear in the upper pane.

In order for this feature to work, there must be an interactive user logged in at the remote machine.

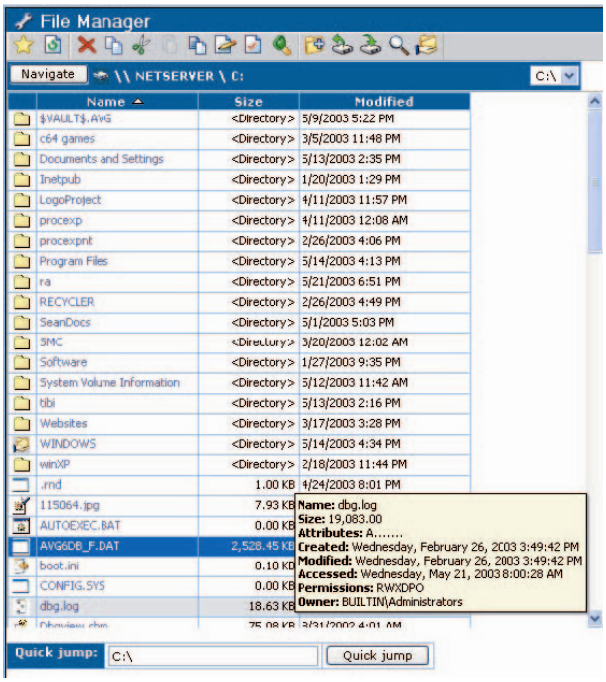
This functionality is implemented in either an ActiveX control or Java applet. RemotelyAnywhere attempts to start ActiveX by default, but will switch to Java if the browser does not support it, or if the Java version is selected in the Help Desk Chat menu.

Computer Management

Under Computer Management you can take advantage of a wealth of RemotelyAnywhere administrative features including the File Manager, data on the Processes, Services and Drivers of the remote machine and rebooting.

File Manager

Clicking on File Manager under System Administration in the menu presents the following interface:



The File Manager displays a list of all available drives, together with their capacity and available space.

Clicking on the drive names will take you into the root directory of that drive, where all files and directories are also links. Clicking on the name of a subdirectory will take you into it and produce a listing. If you click on the name of a file, RemotelyAnywhere will send it to your browser.

You can select multiple consecutive files with the Shift key, or non-consecutive files with the Ctrl key. Then, using the toolbar or by right-clicking you can copy, delete, or move the files. Also:

By clicking **Execute,**  , RemotelyAnywhere will attempt to launch each selected file on the host computer.

The Edit button,  , lets you edit small text files within your browser. This is useful for changing small configuration or batch files without downloading or uploading.

The Attributes button,  , lets you change file attributes, such as Hidden, Read-Only, etc.

The Permissions button,  , lets you specify new Windows NT permissions on the selected objects if the file system supports it.

Clicking the Upload button,  , uploads files to the current directory.

Fields Displayed in the File Manager

- **Icon:** A small icon indicating the file type
- **Name:** File name and extension
- **Attributes:** File attributes (i.e. read-only, system, etc.)
- **Permissions:** Indicates what actions the user can perform on the object (i.e. read, write, change, etc.)
- **Size:** File size
- **Created:** File creation time
- **Last modified:** Last modification time
- **Last accessed:** Last access (read or write) time
- **Owner:** The owner of the file

The following properties are also displayed as tooltips:

- The name of the application that might have this file open
- If the file system supports compression
- The amount of space the file takes up on disk and also the effectiveness of compression, if applicable

The Quick Jump field accepts a path name. Entering a directory (for example C:\Winnt\System32\Drivers) and clicking on the Quick Jump button will immediately take you to the requested location, without having to click your way there. This can be helpful over slow connections.

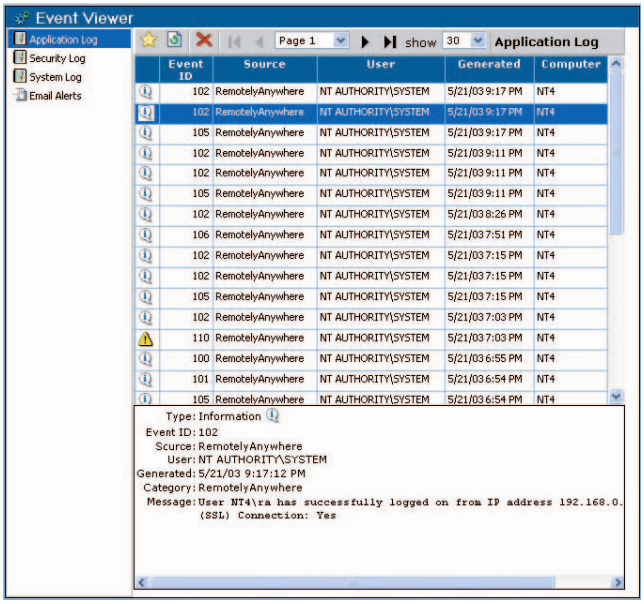
Clicking on header fields will change the sorting order of the file list to the relevant column. For example, to sort files by modification time rather than name, simply click on the header field for that column. To sort in descending order, click the header field of the currently active sorting field again.

User Manager (Vista/XP/2000/NT4 only)

Clicking on **User Manager** under System Administration in the menu you will be able to access RemotelyAnywhere's comprehensive User Manager feature. This supports all the features of NT's built-in User Manger.

Event Viewer (Vista/XP/2000/NT4 only)

If you select Event Viewer under Computer Management in the left-hand menu you can view the NT logs of the remote machine.



This feature is very much like NT's Event Viewer.

You are able to view a listing of log entries on your screen. Clicking on an entry will display its details.

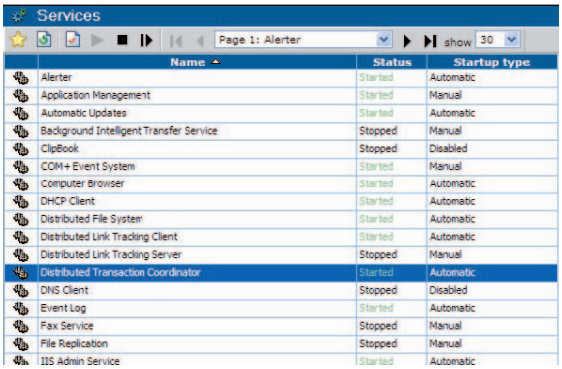
You can choose to clear the contents of the log file by pressing the Delete button in the toolbar. If you specify a filename, the event log will be backed up before being erased.

You can also have RemotelyAnywhere send email alerts to a specified email address when log entries matching a given criteria are entered into any of the event logs.

See the **Scheduling & Alerts > Email Alerts** section of this guide for more information on this feature and its uses.

Services & Drivers (Vista/XP/2000/NT4 only)

When you click on Services or Drivers under Computer Management you will see this information displayed:



The format of the Services and the Drivers lists are identical. These lists display the names and statuses of all the services (or drivers) installed on the remote machine.

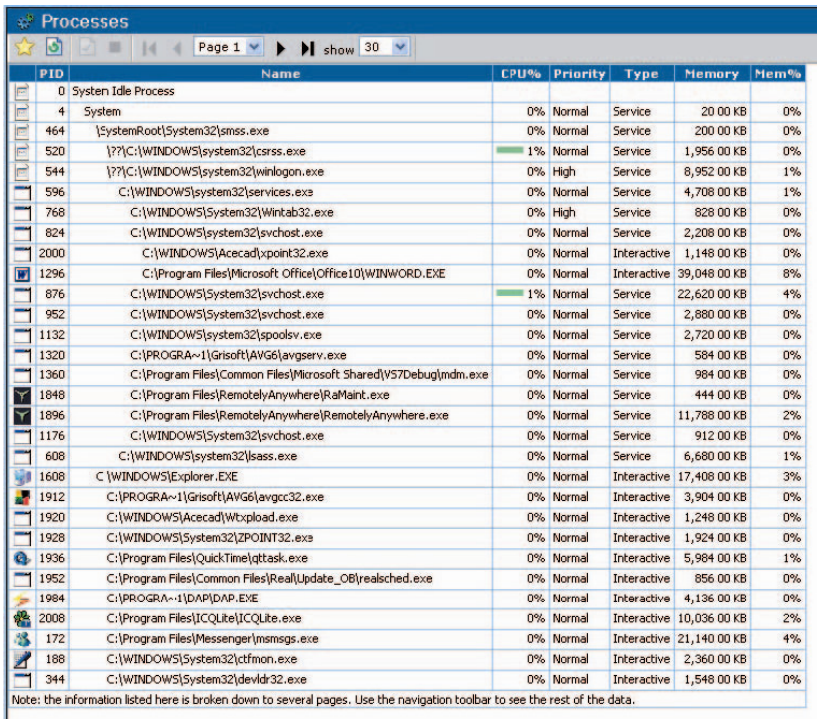
Clicking on the name will show you more detail about the selected object and allows you to control it. You can also change its startup options. When specifying a user account to be used by a service, it must be in DOMAIN\USER form. If you want to use a local user account, you can type .\USER.

In the list of objects, the status field shows Stopped, Running, Starting, Stopping, etc. RemotelyAnywhere looks through the list of services and drivers, and if it finds one that is set to start automatically but is not running, their status will be shown in red. This alerts you to the fact that the service should be running, but isn't.

By selecting a service you can drill down and find out more about its properties as well as starting, stopping or restarting them.

Processes

When you click on Processes under Computer Management in the left side menu the Processes window appears:



PID	Name	CPU%	Priority	Type	Memory	Mem%
0	System Idle Process					
4	System	0%	Normal	Service	20 00 KB	0%
464	\SystemRoot\System32\smss.exe	0%	Normal	Service	200 00 KB	0%
520	\??\C:\WINDOWS\system32\csrss.exe	1%	Normal	Service	1,956 00 KB	0%
544	\??\C:\WINDOWS\system32\winlogon.exe	0%	High	Service	8,952 00 KB	1%
596	C:\WINDOWS\system32\services.exe	0%	Normal	Service	4,708 00 KB	1%
768	C:\WINDOWS\System32\Wintab32.exe	0%	High	Service	828 00 KB	0%
824	C:\WINDOWS\system32\svchost.exe	0%	Normal	Service	2,208 00 KB	0%
2000	C:\WINDOWS\Acecad\xpoint32.exe	0%	Normal	Interactive	1,148 00 KB	0%
1296	C:\Program Files\Microsoft Office\Office10\WINWORD.EXE	0%	Normal	Interactive	39,048 00 KB	8%
876	C:\WINDOWS\System32\svchost.exe	1%	Normal	Service	22,620 00 KB	4%
952	C:\WINDOWS\System32\svchost.exe	0%	Normal	Service	2,880 00 KB	0%
1132	C:\WINDOWS\system32\spoolsv.exe	0%	Normal	Service	2,720 00 KB	0%
1320	C:\PROGRA~1\Grisoft\AVG6\avgserv.exe	0%	Normal	Service	584 00 KB	0%
1360	C:\Program Files\Common Files\Microsoft Shared\VS7Debug\mdm.exe	0%	Normal	Service	984 00 KB	0%
1848	C:\Program Files\RemotelyAnywhere\RaMaint.exe	0%	Normal	Service	444 00 KB	0%
1896	C:\Program Files\RemotelyAnywhere\RemotelyAnywhere.exe	0%	Normal	Service	11,788 00 KB	2%
1176	C:\WINDOWS\System32\svchost.exe	0%	Normal	Service	912 00 KB	0%
608	C:\WINDOWS\system32\lsass.exe	0%	Normal	Service	6,680 00 KB	1%
1608	C \WINDOWS\Explorer.EXE	0%	Normal	Interactive	17,408 00 KB	3%
1912	C:\PROGRA~1\Grisoft\AVG6\avgcc32.exe	0%	Normal	Interactive	3,904 00 KB	0%
1920	C:\WINDOWS\Acecad\Wtxpload.exe	0%	Normal	Interactive	1,248 00 KB	0%
1928	C:\WINDOWS\System32\ZPOINT32.exe	0%	Normal	Interactive	1,924 00 KB	0%
1936	C:\Program Files\QuickTime\qttask.exe	0%	Normal	Interactive	5,984 00 KB	1%
1952	C:\Program Files\Common Files\Real\Update_OB\realsched.exe	0%	Normal	Interactive	856 00 KB	0%
1984	C:\PROGRA~1\DAP\DAP.EXE	0%	Normal	Interactive	4,136 00 KB	0%
2008	C:\Program Files\ICQLite\ICQLite.exe	0%	Normal	Interactive	10,036 00 KB	2%
172	C:\Program Files\Messenger\msmsgs.exe	0%	Normal	Interactive	21,140 00 KB	4%
188	C:\WINDOWS\System32\ctfmon.exe	0%	Normal	Interactive	2,360 00 KB	0%
344	C:\WINDOWS\System32\devldr32.exe	0%	Normal	Interactive	1,548 00 KB	0%

Note: the information listed here is broken down to several pages. Use the navigation toolbar to see the rest of the data.

The output of this function gives you a listing of all processes running on the remote computer.

The list is hierarchical: a parent process will have its child processes listed beneath it, with indentations indicating relationships. Please note that this is for information purposes only, since Windows reuses process IDs.

The following information is available either in the list, by clicking on an item or as tooltips:

PID: The internal Windows NT Process ID.

Name: The name of the executable file with full path. This works as a link, and clicking on it will give you some very detailed information on the process. On that page, you have the option of changing the priority class or the processor affinity for the selected process. This data is arranged under the following tabs for easy viewing: General, Threads, DLLs, Open Files, Registry Keys in Use.

Version: The version of the program, if given.

Description: The description of what the program does, if given.

Memory Used: The amount of memory in use by the process in kilobytes.

Created: The date and time the process was started.

CPU Time: The amount of CPU time (d hh:mm:ss) the process has used.

Priority: The priority class of the process.

Type: The type of the process (service or interactive).

Account: The user account the process runs under.

End Process: The selected process will be terminated immediately.

Selecting **Refresh** retrieves and displays the latest process list.

Registry Editor

This option **(System Administration > Registry Editor)** enables you to edit the registry of the host computer. First, the registry roots (HKCR, HKCU, HKLM, etc.) are displayed, and you can drill down into them by clicking on their names.

Registry keys are displayed in a hierarchical tree. Key values are also displayed, with their name, type and value.

You can edit values that are of either text (REG_SZ, REG_EXPAND_SZ or REG_MULTI_SZ) or integer (REG_DWORD) type and REG_QWORD type values. Binary, etc. values are displayed but cannot be edited.

Using the buttons in the toolbar you can add a subkey, add a value or delete the currently opened key.

Command Prompt

You can access a command prompt from within your browser by selecting Command Prompt under Server Functions in the menu. The Telnet client, written as a Java applet, provides encryption and data compression for security and speed. The Telnet and SSH server included with RemotelyAnywhere lets you access a command prompt on a remote computer from terminal emulator software or a web browser.

You can either use the Java Telnet client that's part of RemotelyAnywhere, or any other terminal emulator you like.

There are several reasons to keep using the RemotelyAnywhere client:

- **It is secure: I**t uses the same encryption that's employed by the remote control module.
- **It's fast**: It uses sophisticated data compression to achieve high throughput.
- You are able to transfer keystrokes that terminal emulators cannot handle, such as the Alt key.
- You can also use your mouse in console applications that support it.

If you decide to use a terminal emulator, you will need to connect to the Telnet port (23) or the SSH port (22). You can change the default listener ports in the configuration dialog boxes to any available port. Should you need to send a special keystroke to the server, press Ctrl-Q and a virtual keyboard will pop up. You can then move the pointer over the desired key with the cursor keys, and press Enter to select it. If you want to send a combination of several keys at the same time, you can select the keys with the Spacebar, and then press Enter after selecting the

last key of the combination.

When a connection is initiated from a terminal emulator, you will be asked to log on.

This is handled automatically by SSH clients, so you need to enter your username and password in the SSH client itself. RemotelyAnywhere currently supports the SSH1 and SSH2 protocols with password authentication. To specify a Windows NT/2000 domain, you can enter it as part of the username, separated from the actual login name with a backslash character. For example: DOMAIN\Username.

With Telnet clients, you need to enter your credentials in clear text during the session. You are asked for your username, password, and Windows NT/2000 domain.

After successfully logging in, you will be asked if you want full console support. If you decline, you will only be able to use stream-mode programs. Applications that take over the whole console window, such as Edit.com, Norton Commander and the Far file manager will not work. However, if you are only planning to use command-line utilities, you can safely decline and you will be right at the command prompt.

If you answered accept full console support, you will be asked to specify the console window size. A default value is provided for you. You should make sure that the terminal emulator you are using supports it and is set to the size you enter here.

Finally, if you have an ANSI compliant terminal emulator, you can choose to use ANSI color support during the session.

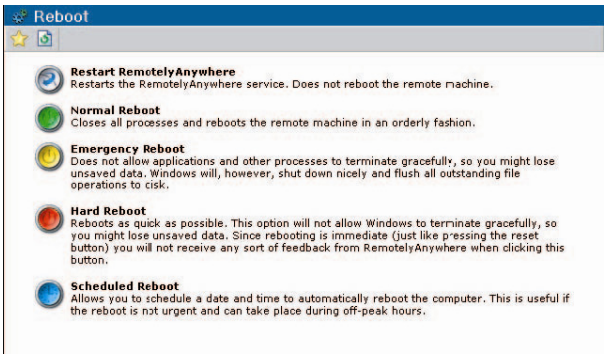
Should you disconnect your terminal emulator or go to a different page in the browser window containing the Telnet client Applet, all applications you have running in the Telnet session are left active.

You can reconnect to this Telnet session by simply logging in (or loading the Applet) again. There is a timeframe for this: if you do not reconnect within an hour, all your Telnet applications, including the command shell, are terminated. You can change the timeout value from the default one hour in the configuration dialog boxes.

To permanently close the Telnet session, type exit at the command prompt.

Reboot

When you click on Reboot under System Administration in the left menu you will see the following window:



With this feature you can reboot the machine. You have the following choices:

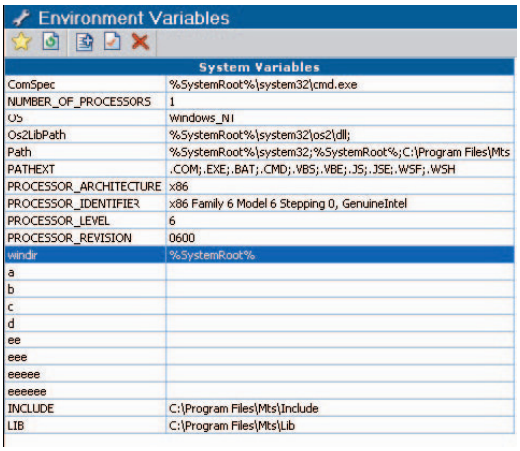
- **Restart RemotelyAnywhere:** Restarts the RemotelyAnywhere service. It does not reboot the remote machine. This is useful if you change settings like the listening port and have no physical access to the machine in order to restart the service.
- **Normal Reboot:** Closes all processes and reboots the remote machine in an orderly fashion.
- **Emergency Reboot:** Does not allow applications and other processes to terminate gracefully, so you might lose unsaved data. Windows will, however, shut down nicely and flush all outstanding file operations to disk. This can be useful if there are hung processes that prevent NT from shutting down normally.
- **Hard Reboot:** Reboots as quickly as possible. This option will not allow Windows to terminate gracefully, so you might lose unsaved data. Since rebooting is immediate (just like pressing the reset button) you will not receive any feedback from RemotelyAnywhere when clicking this button.
- **Scheduled Reboot:** This allows you to schedule a date and time to automatically reboot the computer. This is useful if the reboot is not urgent and can take place during off-peak hours.

Computer Settings

In addition to the administrative features available under Computer Management, you can also view and modify a number of settings on the remote machine, from Environment Variables to Automatic Priorities.

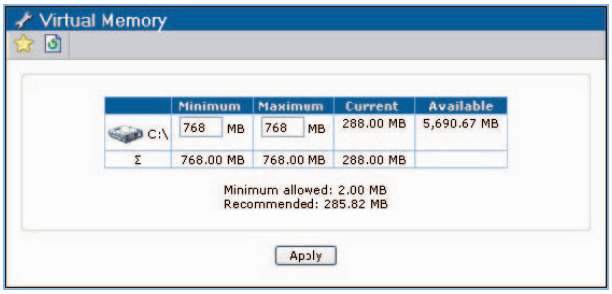
Environment Variables

Here you can view and make any necessary changes to Environment Variables on the remote machine. User environment variables that are defined by you or by programs are listed here, such as a path where files are located:



Virtual Memory

When you click on Virtual Memory under System Administration in the menu this dialog box is displayed:



Here you can change virtual memory settings on the remote computer. Simply enter a minimum or maximum size for the paging file next to the listed drive and click **Apply.** Entering zero values both for the minimum and maximum size will remove the paging file from the drive. You will need to reboot the computer for any changes to take effect.

Time

You can edit the time on the remote computer under Computer Settings > Time. Simply enter the correct values and click the Apply button. Please note that the time is displayed according to the time zone settings of the host computer.

Automatic Login

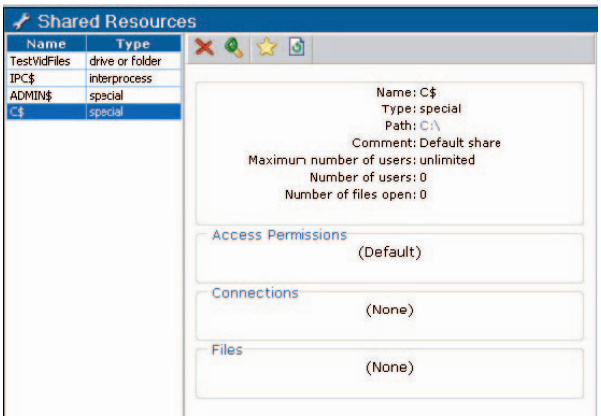
This option lets you enable or disable NT's autologon feature. You can also do this via the Registry or with other small utilities, like the one included in the NT Resource Kit.

Enabling autologon will cause the server to bypass the logon screen after system startup and log in with the username and password specified.

Note: This is a potential security risk: the username and password are stored in the Registry in clear-text format.

Shared Resources

When you click on Shared Resources under System Administration in the menu this what you will see:



This function gives a detailed report of all shared resources on the remote computer, including shared folders, administrative shares, and printers.

This screenshot above shows the C$ administrative share. The Path link takes you to the directory in the File Manager. The connections list shows open files, if any, and these files can be closed forcibly by clicking **Close.**

Access permissions active on the object are also shown in detail, except for administrative shares where permissions cannot be set.

The Delete Share button removes sharing from the object.

Automatic Priorities (Vista/XP/2000/NT4 only)

Automatic Priorities **(System Administration > Automatic Priorities)** lets you direct RemotelyAnywhere to automatically change process priorities.

If you have ever wished to run a backup on your server without impacting performance, or to archive a huge directory structure using zip/winzip on a live web server without putting additional load on the machine, you will find this feature useful. The same applies if you have ever wanted your workstation to be responsive while you browse the web on your workstation while carrying out a lengthy compile.

Selecting **Automatic Priorities** takes you to a dialog box that displays a list of executables and their target priorities. By default, the list is empty, so you need to click on **Create** in the toolbar. On the dialog box that appears, enter the name of the executable, and select the target priority from the dropdown box.

> **Note:** The name of the executable is without paths, so, for WinZip it is WINZIP.EXE, for the Microsoft C compiler it's CL.EXE, etc.

The target priority is normally **Idle.** This puts your process in the same priority class as the screen saver, meaning that it will only get a chance to make any progress if it does not compete for CPU power with other processes. You can also select a target CPU for the process. This allows you to divide processes amongst CPUs on an SMP machine to suit your needs. Click **Add** to return to the previous list that displays the name of the executable and the priority class you selected for it.

If there are entries in the above list, RemotelyAnywhere will scan the process list on your machine every ten seconds, looking for the process names you entered. If RemotelyAnywhere finds one and its priority class does not match the one you specified it will be changed to your preference.

Server Functions

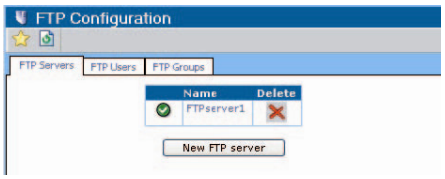
Under Server Functions you can find all the pages you'll need to make use of RemotelyAnywhere's powerful FTP and Port Forwarding capabilities.

RemotelyAnywhere Server Edition comes with an extremely versatile FTP server. You can set up an unlimited amount of FTP servers on one computer, each with its unique IP address and port combination. You can create users and groups for your FTP server, or you can use the built-in Windows NT accounts for rights management.

If logging has been enabled via **Preferences > Log Settings**, the FTP Server will log all user activity to the main RemotelyAnywhere log file.

FTP Configuration

When you click on FTP Configuration under Server Functions in the menu this what you will see:



The options for creating and managing the settings for your FTP servers, users and groups are arranged into three tabs. We will address the content of each tab in turn.

FTP Servers

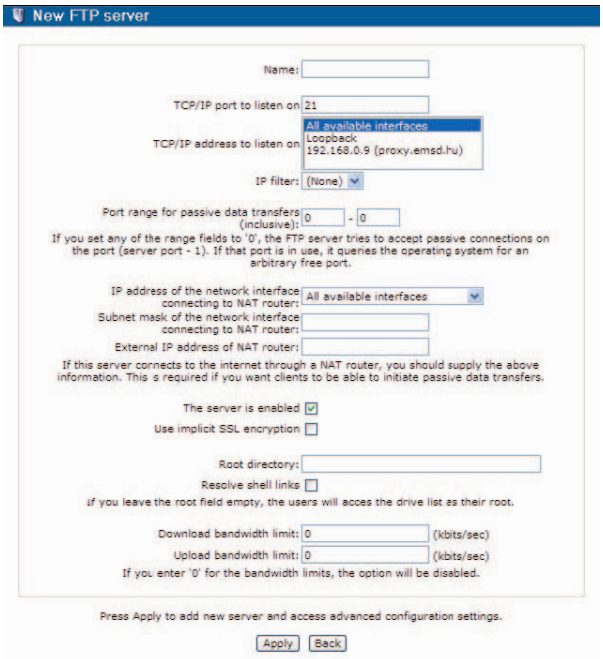
In order to create a new virtual FTP server on your machine you need to define at least one virtual FTP server on the FTP Servers tab of the FTP Configuration screen. If no FTP servers are defined then this screen will be blank, but for the New FTP server button.

Once you have defined a new server it will be shown in a table as in the screen shot above. You can delete a server by clicking on the red cross in the delete column to the right of a given server. The server can be started and stopped by clicking on the status indicator to the left of the virtual server.

A green check mark indicates that the server is running, and a red cross shows that it is stopped. This may be because it was stopped manually, it has been disabled or it was not able to start due to an error.

When you stop an FTP server on this screen its status will change to **Disabled.** This means that when you reboot the computer the server will not be started automatically. Likewise, if you start a stopped or disabled FTP server it will be **Enabled** and will start automatically on rebooting.

New FTP Server: To set up a new FTP server, click on **New FTP server** at the bottom of the FTP servers tab. This will bring up the New FTP server dialog box, which will look something like this:



You can specify the following settings for your new FTP server here:

Name: The name of the virtual FTP server. This is for reference purposes only. You can call your server whatever you want. This is what will be displayed on the FTP configuration screens, the login message from the FTP server, and so on.

TCP/IP port to listen on: The port in use by the virtual FTP server. The default is the standard FTP port, 21.

TCP/IP address to listen on: The IP address to use. You can select one item from the list. If you select All available interfaces the virtual FTP server will listen on all assigned IP addresses.

IP Filter: The IP Filtering drop down lets you specify the IP addresses from which to accept connections. By default, the clients can come from any IP address. The IP filtering engine is the same as that used by RemotelyAnywhere itself. Please see the section on IP filtering under Security for more information.

Port range for passive data transfers (inclusive): This feature is relevant to passive mode data connections (PMDCs),

also known as PASV mode in some clients. In such cases the data channels are opened by the client and the server communicates a PASV reply stating which address and port to connect to. However, servers behind firewalls and/or routers may have problems with the use of the reported address and/or port.

If the server is behind a firewall there may be a problem with the port on which PMDCs are accepted. By default the server tries the port (server port - 1). For example, the server will try port 20 if it is on the default FTP port of 21. If multiple clients were to try to establish simultaneous data connections this would fail and the server would query Windows for an arbitrary free port. Behind a firewall connection to random ports will not work. To avoid this, you can specify a range of ports on which to accept PMDCs. If these ports are open on the firewall then the connection will be established.

IP address of the network interface connecting to NAT router and **External IP address of NAT router:** By default the server examines the local IP address to which the client is connected and accepts the PMDC on that address. In a NAT environment this is likely to fail, because the server's local IP address is not externally visible for access from the Internet. To avoid this we can configure the FTP server to report a user specified IP address instead of the local one, although only for connections passing through the router. Thus we must specify the IP address of the network interface connecting to the router, and that to report to clients opening PMDCs through this interface. This should be the router's external IP address.

Subnet mask of network interface connecting to NAT router: In the above scenario a problem remains, which is that clients connecting from the LAN, possibly using the same network as the router would be redirected to open the PMDC using the external address. Most routers do not support this. Thus there is a third setting which allows you to specify the subnet mask of the network interface. Clients connected from the same subnet as the router will not be redirected. If the subnet parameter is not specified all connections from the interface will be redirected.

A typical FTP server setup behind an NAT router and a firewall

Imagine a machine on which RemotelyAnywhere has been installed with a local IP address of 192.168.1.2 (subnet mask 255.255.0.0) and the external IP address of 123.45.67.89 (belonging to a NAT router/firewall). We would need to do the following in order to set up an externally accessible FTP server on this machine:

1. Create an FTP server within RemotelyAnywhere with the default settings, listening on all available interfaces, with the default FTP port of 21.
2. On the main configuration page of our new FTP server set the IP address of the network interface connecting to the NAT router as 192.168.1.2, the subnet mask to 255.255.0.0, and the external IP address to 123.45.67.89
3. Set the port range for passive data transfers to 5200-5299
4. Configure your router so that it forwards connections to 123.45.67.89:21 to 192.168.1.2:21 and make sure

port 21 is open on the firewall.

5. Configure the router to forward connections to 123.45.67.89:5200-5299 to 192.168.1.2:5200-5299 and make sure that you open the 5200-5299 port range on the firewall.
6. Finish configuring your remaining FTP settings (security, users, etc.)

The server is enabled: If a server is enabled it will start automatically with RemotelyAnywhere. If disabled you will need to start it manually.

Use implicit SSL encryption: Here you can set your new virtual FTP server to use implicit SSL encryption. Please note that if a server uses implicit SSL connections, it will accept these connections alone and clients must be configured accordingly. Most clients default to port 990 when creating implicit SSL FTP site entries.

Root directory: The root directory for the virtual FTP server. If you leave this field blank the drive list will be used as the root.

Resolve shell links: If you enable this option, shell links (.lnk files) pointing to directories will be displayed as directories, enabling you to use Unix and Windows 2000-style hard links.

Download bandwidth limit: The global download speed limit for the server. No matter how fast users are accepting data, the server will not send it any faster than the speed specified here.

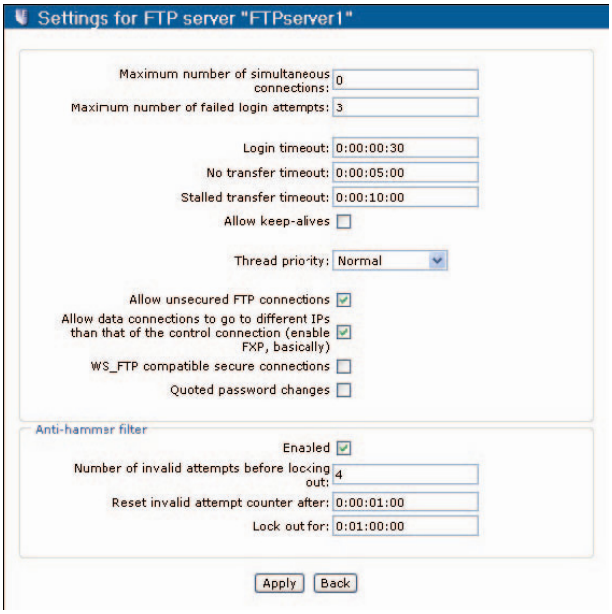
Upload bandwidth limit: The global upload limit to the server. No matter how fast users are sending data, the server will not accept it any faster than the speed specified here.

When you've filled in the required data to define your new server, click apply. The following FTP server configuration pages will become available as buttons at the bottom of the page:

- Security
- NT Users
- Welcome
- ODBC

Security

The Security dialog box lets you specify various security and connection-related options. It will look like this:



Maximum number of simultaneous connections: The maximum number of simultaneous connections to the FTP server. Setting it to zero means that there are no limits.

Maximum number of failed login attempts: If a user fails to log in with the specified number of tries the connection will be dropped.

Login timeout: The maximum number of seconds the user can take to log in.

No transfer timeout: The connection will be considered idle and will terminate after the specified number of seconds have elapsed on an open connection without a file transfer or directory listing.

Stalled transfer timeout: This is the amount of time a file transfer can spend without sending or receiving any data before it is considered stalled and thus terminated.

Allow keep-alives: FTP clients use various commands to keep the connection from being idle. When enabled, FTP commands such as CWD, PWD or the ubiquitous NOOP will reset the No transfer timeout counter (described above). If disabled, only an actual file transfer or a directory listing will reset the counter.

Thread priority: You can select the priority of the threads servicing users for the FTP server. If you are running an FTP server on an otherwise busy web server it might be a good idea to set the priority to a lower value than the default Normal setting.

Allow unsecured FTP connections: If this option is disabled the FTP client must support and utilize SSL.

Allow data connections to go to different IPs than that of the control connection (enable FXP, basically): The FTP protocol uses two connections: The control connection and the data connection. The data connection is where all the raw data is sent, the control connection is used to send commands to the server and receive replies. Normally data connections are set up to the same IP address as that of the control connection, but in order to facilitate server-to-server file transfers it may be desirable to allow data connections to go to different IP addresses. If you are not using server-to-server transfers you can safely disable this option.

Quoted password changes: This determines whether the parameters of the SITE PSWD command are in quotes or simply surrounded by a space. (SITE PSWD oldpwd newpwd vs. SITE PSWD "oldpwd" "newpwd").

Which form is used depends on the targeted FTP client.

Anti-hammer filter: This feature is similar to RemotelyAnywhere's IP address lockout settings. By default if 4 bad logins occur from an IP address within one minute, the IP address will be locked out for one hour.

Number of invalid attempts before locking out: You can change the number of bad login attempts from 4 to anything you want.

Reset invalid attempt count after: You can modify the time before the invalid attempt count is reset to zero.

Lock out for: You can choose the duration for which the user is locked out after the specified number of invalid attempts has been made.

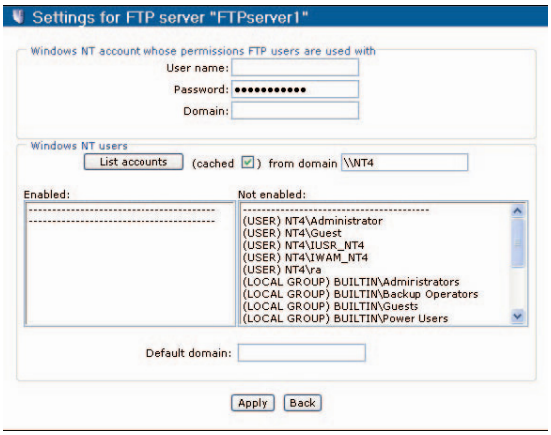
NT Users: You can connect to the newly defined FTP server with any FTP client, but you are not able to log in until you have created a new FTP user and give them access to the server or you can allow any Windows NT user to access the new virtual FTP server.

The difference between FTP users and NT users is simple:

NT users are pre-existing users in the Windows NT user database. Creating and managing them is done via the User Manager – either the HTML-based one included in RemotelyAnywhere, or the User Manager applet that comes with Windows. You cannot explicitly tell the FTP server the directories and files to which the user has access, but Windows access rights will be enforced. If a user can access a file below the server's root directory locally or over the network, he will be able to do so via FTP as well. If a user has no rights to a file or a directory, he will not be able to access the object with FTP either. This is enforced by the FTP server by having the thread servicing the user impersonate him towards the operating system as soon as login is complete.

FTP users, on the other hand, are created and managed within the FTP configuration pages. You can tell the server which files or folders the user can access, where he can read from, where he can write to. When an FTP user logs on, the thread servicing the user is executing under the LocalSystem account by default. This is rather undesirable, so you can specify an NT user account on a per-server basis that will be impersonated when servicing FTP users. We will return to FTP users later in this chapter, when discussing the content of the FTP users tab.

Clicking **NT Users** will bring up the following dialog box:



The Windows NT account whose permissions are assigned to FTP users fields let you specify a username, domain and password for an existing Windows NT account. This is used when an FTP user logs on: the thread servicing the user will be impersonating this account towards the operating system. If you enter an incorrect username or an incorrect password here, the FTP user will receive a 'Login incorrect' message from the FTP server, even if he enters his credentials correctly.

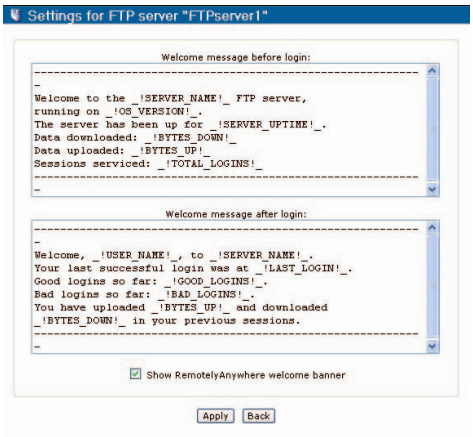
To grant access to a Windows NT user or group on the FTP server, select its name in the list in the right pane and click the Update button. To revoke access from a user or a group, select its name in the list on the left, and click the Update button.

To list user accounts from a domain rather than from the local computer, enter the domain's name in the **Default domain** field and click **Update.**

Now that you have granted access to an NT user, you can use an FTP client to connect and log in to the FTP server. The user will have access to all files and directories below the server's root directory. However, on an NTFS file system, NT access restrictions will apply. For example, if the user does not have the rights to read or write in a certain directory, he will not be able to do so via FTP either. The FTP server enforces this in a very effective way: the thread servicing the user will impersonate him towards the operating system as soon as login is successful.

Welcome

The Welcome dialog box allows you to view and modify the welcome message your users see:



The first message the user will see when they log in will be the RemotelyAnywhere welcome banner. If you do not wish to let the outside world know which FTP server you are running, you can disable this via the checkbox at the bottom of this window.

The next message the user will see is by default:

> ---
>
> Welcome to the _!SERVER_NAME!_ FTP server,
>
> running on _!OS_VERSION!_.
>
> The server has been up for _!SERVER_UPTIME!_.
>
> Data downloaded: _!BYTES_DOWN!_
>
> Data uploaded: _!BYTES_UP!_
>
> Sessions serviced: _!TOTAL_LOGINS!_
>
> ---

You can change this to anything you like, or leave it blank if you'd prefer no login message for your users. If you disable both the banner and the welcome note, the FTP Server will just send 'Welcome' whenever somebody connects to the FTP port. This is because the FTP specification requires a server to send a code and some text when a connection is established.

By default, the post-login message is:

Welcome, _!USER_NAME!_, to _!SERVER_NAME!_.

Your last successful login was at _!LAST_LOGIN!_.

Good logins so far: _!GOOD_LOGINS!_.

Bad logins so far: _!BAD_LOGINS!_.

You have uploaded _!BYTES_UP!_ and downloaded

_!BYTES_DOWN!_ in your previous sessions.

User logged in.

The final line: **User logged in** cannot be customized, as this is a requirement of FTP protocol. The rest you can change to suit your preferences, or leave blank.

The following variables can be inserted into the welcome messages, and they will be automatically replaced with their corresponding values:

_!SERVER_NAME!_

The name of the FTP server.

_!OS_VERSION!_

The operating system and its version.

_!SERVER_UPTIME!_

The amount of time the server has been up.

_!BYTES_UP!_ and _!BYTES_DOWN!_

The amount of data uploaded and downloaded. These variables behave differently when used in the pre-login or post-login messages. In the pre-login message, they represent a server-wide value, while in the post-login message they represent the amount of data transferred by the user.

_!TOTAL_LOGINS!_

The number of successful logins to the FTP server. Only valid in the pre-login message.

_!GOOD_LOGINS!_ and _!BAD_LOGINS!_

The number of logins and unsuccessful login attempts. Only valid in the post-login message.

_!LAST_LOGIN!_

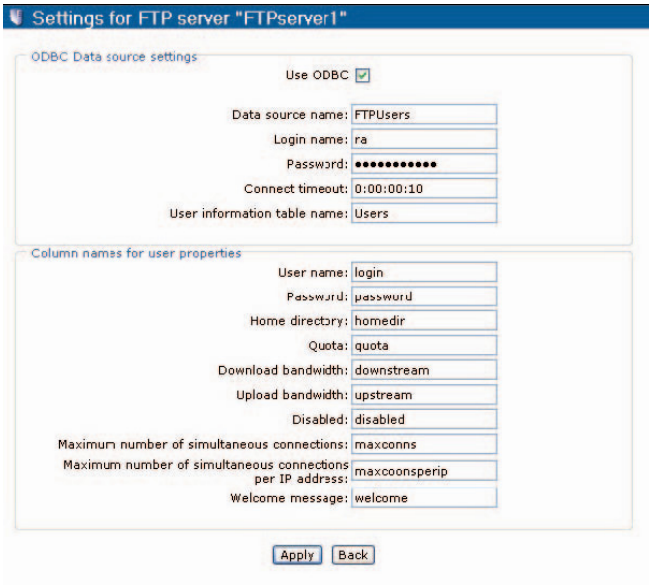
The last successful login by the user. Only valid in the post-login message.

These welcome messages are server-wide settings, and apply to all users and groups. When you specify a welcome message for an FTP group or an FTP user, it will override the post-login message defined here.

ODBC Access

The ODBC option allows you to specify a database as a source of user information as in the image on the next page.

With this dialog box you can set up a database to contain user information. This can be any database type: Oracle, SQL Server, Microsoft Access, or even a plain text file. You need to create an ODBC data source that refers to this database so that RemotelyAnywhere can access it. The data source must be a so-called Machine Data Source, as this is the only ODBC source available to processes running in the system context.



When you have your database and ODBC data source ready, we advise you to test it by querying it with a tool that supports ODBC queries, such as a spreadsheet program.

You should have all user information available in one table. If you already have a user database and user information is in separate tables, you should set up a query within your database that contains all user-related fields. RemotelyAnywhere only reads from the database.

The above screenshot is set up for the following scenario:

Suppose that you have a user database in a data source called FTPUsers. The user information is present in a database table called Users. A database user called ra is able to read from the Users table. You should also supply the password for this user in the above form.

The Users table can have any number of fields in any order, but the above figure assumes that these fields are

present:

login (character string)

password (character string)

homedir (character string)

quota (integer, in bytes, optional)

downstream (integer, speed in bytes/sec, optional)

upstream (integer, speed in bytes/sec, optional)

disabled (integer, zero or non-zero, optional)

maxconns (integer, optional)

maxconnsperip (integer, optional)

welcome (character string, optional)

The only three mandatory fields are **login, password and homedir.** The login and password fields contain the user's login name and password, in clear text. The homedir field must contain the user's home directory, which can be an absolute path (such as z:\ftp\users\~john) or it can be relative to the server root (such as /users/~john).

Users have full access to their home directory, but have neither read nor write permissions outside of it.

The **quota** field will not let the user store more data in his home directory and its subdirectories than the number of bytes specified here.

The **downstream and upstream** fields restrict download and upload speed. They are optional, and should be an integer number specifying bytes per second.

The **disabled** field should be an integer. When it's non-zero, the user is disabled and cannot log in.

The **maxconns** field specifies the maximum simultaneous connections to this FTP server for a user.

The **maxconnsperip** field specifies the maximum simultaneous connections per unique IP address for a user.

The **welcome string**, if used, should contain a custom welcome message for the user.

FTP Users

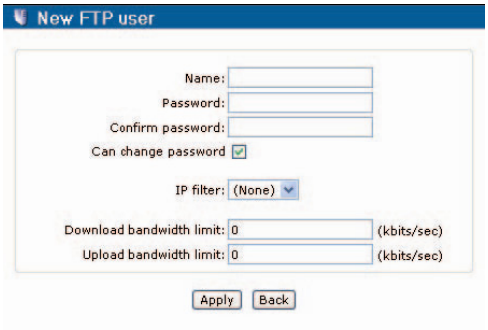
If you click on the FTP users tab; **Server Functions > FTP Configuration** you can view, create or modify your existing FTP users. These are only defined in RemotelyAnywhere and unlike NT users they do not exist outside of the FTP server.

As on the FTP Servers page, users are shown in a table, with a delete column to the right.

Below this is the New FTP user button.

New FTP User

To create a new FTP user click on the New FTP user button on the FTP Users tab of the FTP configuration page.



Enter the desired username and password in the above dialog. You can also specify upload and download speed limits for the user. If not set to zero (meaning disabled) these options override the global FTP server settings.

You can also enable or disable their ability to change this password, and select an IP from the IP filter drop down menu. Click **Apply** to create the user.

When you create a new user the following options become available:

Groups

Permissions

Ratio

Disable

Home/Quota

Max Connections

Welcome

Permissions Report

The newly created user cannot log in yet: you have to assign permissions to them for an FTP server and a path so that the user is able to use the account.

To allow anonymous access to an FTP server, you should create an FTP user called anonymous. This user account is special: no password checking is done upon login. You can assign permissions to the anonymous user account as you would to any other user. By default, the newly created anonymous user has no rights to any virtual FTP server defined.

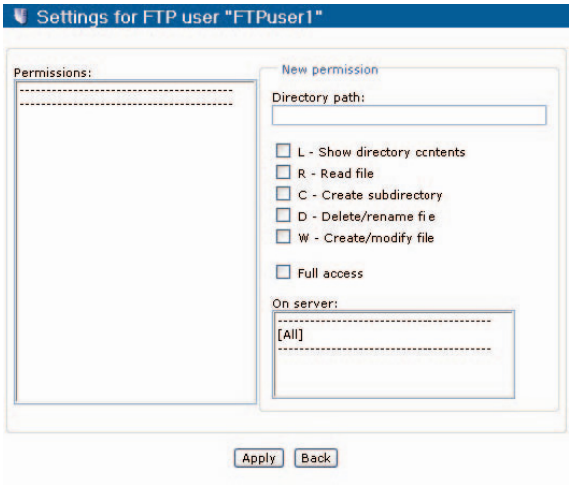
Groups: This dialog box lets you specify the FTP groups to which the user belongs. For more details on FTP groups, please see the next section.

Selecting a group that the user is a member of and clicking the Update button will remove the user from that group. Selecting a group that the user is not a member of and clicking the Update button will add the user to that group.

The Back button takes you back to the main user editing dialog box.

Permissions

The following dialog box lets you edit users' access to directories:



This dialog box lets you edit users' access rights to directories. To grant access to a directory on a server, select the virtual server from the server list, select the type of rights you wish to assign to the user, enter the path to the directory and click the Update button.

The path you specify can be a full path, containing a drive letter, or a path relative to the server's root directory. If you assign rights to a path that is not within the server's root directory, the setting will have no effect at all.

The following rights are possible:

L – Show directory contents: Allows the user to list the contents of the directory.

R – Read file: Download files from the directory.

C – Create subdirectories: Create new directories in the directory.

D – Delete/rename file: Delete or rename a file or a directory. Also required to be able to overwrite files.

W – Create/modify file: Create a new file and/or write data to it.

Full access: All of the above.

The above settings let the user access FTP Server 1 – he has full control over the contents of the server. These rights only apply to the root directory of the server and all directories below that. The user also has list, read and write access to the c:\work directory on FTP Server 2. However, the user has no rights at all to the c:\work\java directory on FTP Server 2. The user has no rights at all on FTP Server 3, meaning he cannot even log on.

The rights you specify for a directory are automatically inherited by its subdirectories, unless you specify different rights for them.

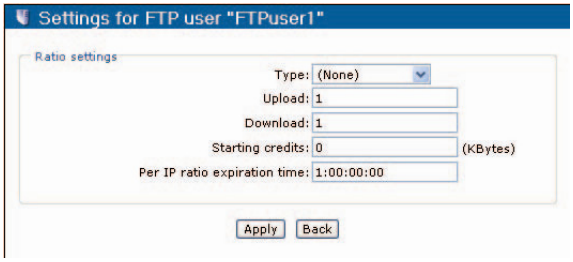
The following method is used when checking access rights to a directory:

1. The current virtual server's access list is enumerated for the current user.
2. When the directory closest to the directory in question is found, the access rights specified for that directory is used. For example, if the user has LRW rights for C:\Work, he has LR rights for C:\Work\CPP, and the directory in question is C:\Work\CPP\Project1, only LR rights are returned – meaning that the user can only list and read files, but not write to them.
3. If an NT user is specified for the server to run FTP accounts under, further Windows NT-enforced restrictions might apply, based on file system permissions.

You can also make the user member of one or more groups, and these groups can also be members of one or more groups. For an explanation of this scenario, please see the FTP Groups section of this document.

Ratio

This dialog box lets you edit the upload/download ratio settings for the user:



The upload and download ratios let you control how much data the user has to upload before being allowed to download anything.

If the Upload ratio is set to 1, and the Download ratio is set to 5, the user can download 5 bytes for every byte uploaded. If it were vice-versa, the user would have to upload 5 bytes to be able to download one. You can enter any positive integer number in either of these fields.

There are four possible settings for the Ratio type:

1. **None:** The user is a normal user, and can download any file he has read access to, without having to upload first.
2. **Per session:** When the user logs in, his counters are zeroed. Should he lose connection while uploading or downloading, any remaining credits he has will be lost.
3. **Per user:** The user's credits are remembered over sessions. It is not recommended if you want several users to share the same account.
4. **Per IP:** Even if the user loses connection, his credits are remembered, if he logs in again from the same IP address. This does not cause a problem, even if the user account is shared by hundreds of concurrent users.

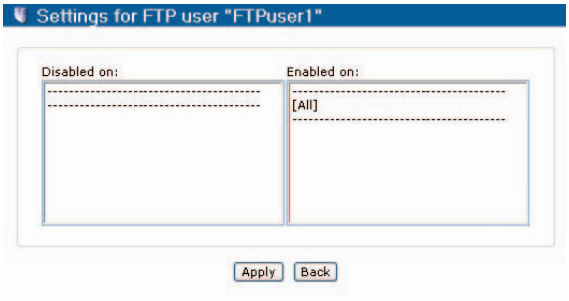
The Per IP ratio information expiration time setting allows you to have the per-IP credits expire after a certain time. If the user logs back from the same IP address after not visiting the server for the specified time, he will have to start building up credits again.

The ratio setting applies to all virtual servers.

To let the user download files without uploading, you can specify a starting credit. The amount given is in kilobytes – the user will be able to download the specified amount of data without uploading.

Disable

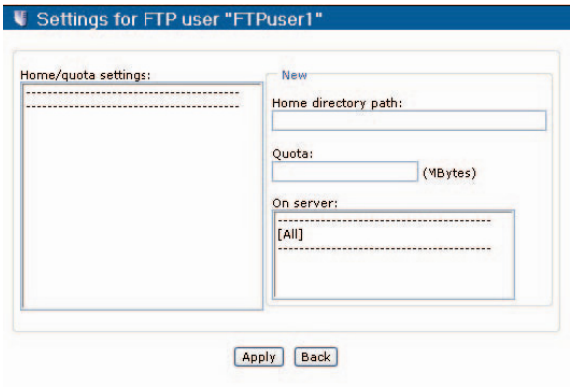
This dialog box lets you explicitly disable (or ban) a user on a virtual FTP server:



Disabled users cannot log in, even if they have rights on an FTP server. You can also disable a connected user from the FTP status page.

Home/Quota

This dialog box lets you specify home directories for the user.



A home directory is basically the entry point for a user on an FTP server. When the user logs in, he will find himself in the directory you specify. If no home directory is specified, he will be logged in to the server's root directory. The user can move out from his home directory if he has rights to an outside directory.

You can use a full path, starting with a drive letter, when specifying home directories – or you can enter a relative path to the server's root directory. Home directories specified above the server's root directory are disregarded.

You should make sure that the user has rights to his entry point on the server – either to his home directory, or if the home directory is not specified, to the root directory of the server. If the user has no rights to the entry point, he will not be able to log in.

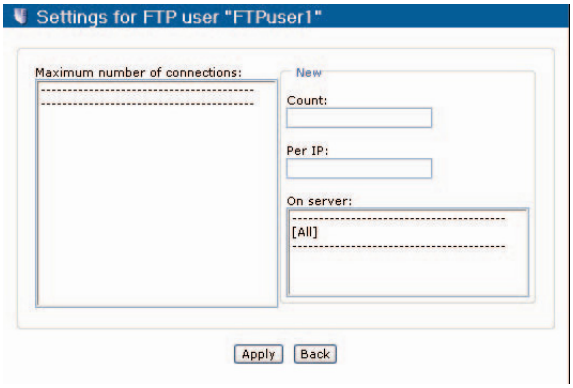
You can specify quotas for your users. Quotas are only enforced on home directories, and apply to all files contained in the home directory and its subdirectories. If a user has rights to upload files outside of his home directory, he will be able to do so without restrictions – quotas only apply to the home directory and its contents.

Since Windows does not support disk quotas for user accounts, RemotelyAnywhere has to enforce them. When a user starts to upload a file, the FTP server quickly scans the contents of the directory to determine if the user is below or above the quota. If the quota is not exceeded, the upload can be started – however, the FTP server will interrupt the transfer as soon as the file being uploaded starts to exceed the specified quota.

Home directory quotas are entirely optional, by leaving the field empty you choose not to limit the amount of data that can be stored on the server by the user.

Maximum Connections

You can specify the maximum number of simultaneous connections for a user account in this dialog box:



By default, a user account can be used to log in any number of times, until exhausting the maximum number of connections for the virtual FTP server, or exhausting the resources of the computer.

Simply select the server on the right, enter the number of maximum simultaneous connections in the **Count** field and click **Apply**. To remove a limitation, select it in the list on the left and click **Update.**

You can also limit the number of simultaneous connections for the user from a computer or IP address. The Per IP field serves this purpose. When left blank, or a zero is entered, this limitation is disabled. If you enter a numeric value, a single computer can be used to log in that many times with the account.

It is a good idea to limit certain user accounts (for example the Anonymous account) this way. An overall maximum connection limit ensures that the server cannot be overloaded by thousands of Anonymous users, and a Per IP limitation makes sure that no single user can take up all available connections.

Welcome

You can compose a custom welcome message for the user in this window.

Welcome, _!USER_NAME!_, to _!SERVER_NAME!_.

Your last successful login was at _!LAST_LOGIN!_.

Good logins so far: _!GOOD_LOGINS!_.

Bad logins so far: _!BAD_LOGINS!_.

You have uploaded _!BYTES_UP!_ and downloaded

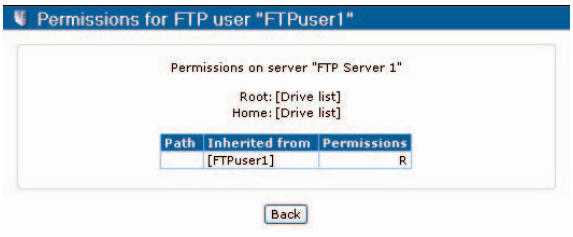
_!BYTES_DOWN!_ in your previous sessions.

!QUOTA!

Messages specified here override any post-login message specified for the virtual FTP server. In this case, messages specified for any groups the user belongs to will be disregarded as well. See the equivalent section on welcome messages above for the available variables.

Permissions Report

The permissions report can be retrieved for any FTP user. It will list all FTP servers, and all the rights a user has on the given server. Here is a sample report for a user on FTP Server 2:



You can see that the user can list, read and write to files in the C:\Work directory. The Inherited from column shows that this particular right was granted to the user himself.

The user has full access to the C:\Work\files directory, due to being a member of the filexfer group. As a member of the web group he also as full access to the C:\Work\websites directory.

He has no rights at all to the C:\Work\Java directory – and it is clear that the user himself has been denied access.

This report can be useful if you have a more complicated setup of groups and users, and would like to see what exactly the user can do on the system, and from where these rights come.

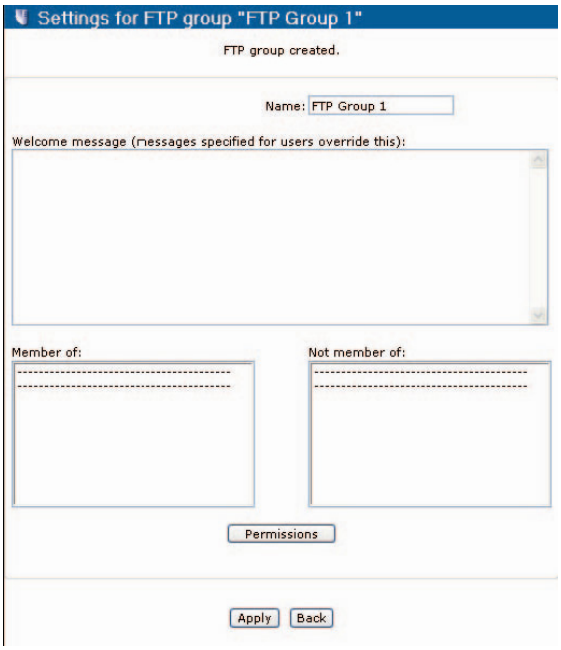
FTP Groups

If you click on the FTP Groups tab via **Server Functions > FTP Configuration** you can easily control the resources available to your FTP users. As on the FTP Servers and Users pages, groups are shown in a table, with a delete column to the right.

To add a new FTP Group, click on New FTP Group.

General Group Settings

This dialog box lets you specify general settings for a group:



You can make a group a member of another group, thus bringing in any permissions or restrictions for its member users from the parent group.

Selecting a group in the Member of list and clicking the Update button will remove it from that group. Selecting a group in the Not member of list and clicking the Update button will add the group to it.

You can also specify a welcome message for a group. Whenever a member logs in, he will see this message instead of the server's general welcome message.

Permissions

With this dialog box you can specify the rights to servers and directories. It works very much like the FTP User Rights dialog box. For a basic description please see the appropriate section of this document.

There are some scenarios, however, that might require further explanation:

Let us examine the following, rather complicated scenario:

- User1 is member of Group1.
- Group1 is member of Group2 and Group3. On the membership display, Group2 is shown first and Group3 is shown second.
- User1 is granted LR access to C:\, and LRW access to C:\Work.
- Group1 is granted full access to C:\, LR access to C:\Work, and LRWD access to C:\Work\CPP.
- Group2 is granted LR access to C:\Work\CPP and full access to C:\Work\CPP\Project1
- Group3 is granted LR access to C:\Work\CPP\Project1

So, what exactly can User1 do in the aforementioned directories?

- **C:** He has LR rights. He was explicitly granted LR rights to this directory, and this overrides anything else.

- **C:\TEMP** He has LR rights. He was explicitly granted LR rights to the directory closest to this one (C:\), and no groups that he is a member of, directly or indirectly, specify anything else for the C:\TEMP directory.

- **C:\Work** LRW rights again. See the first case.

- **C:\Work\CPP** LRWD, because Group1 has LRWD rights. Even though Group2, which Group1 is a member of, specifies LR access for this directory, Group1 is the least indirect object that specifies actual rights for the directory. Group2 is one more indirection away, with User1 only being a member of it because he is a member of Group1, and is therefore overridden by Group1.

- **C:\Work\CPP\Project1** Full access. Both Group2 and Group3 are two indirections away, they both specify access rights to the same directory, so the deciding factor between Group2 and Group3 is that Group2 is the first one in the list on the membership display of Group1.

FTP Status

When you click on **FTP Status** under Server Functions in the menu you can view the current status of each of your virtual FTP servers.

For each server, it provides a listing of all current connections and their current activity. The fields in the list are:

Icon: This field shows a small icon, representing the current status of the connection. A green checkmark indicates a ready, or idle connection. An hourglass indicates a connection currently in the process of logging in or becoming ready. An up or down arrow indicates uploading or downloading.

User name: The name of the user associated with the connection. For NT users, it is in an AUTHORITY\ACCOUNT form. For FTP users, it's simply the username. For connections not yet logged in, it's N/A.

Control address: The IP address of the FTP control connection.

Downloaded Bytes: downloaded during this connection.

Uploaded Bytes: uploaded during this connection.

Data address: The IP address of the FTP data connection, if applicable.

Path: The path and name of the file currently being uploaded or downloaded, if any.

Speed: The speed of the upload or download process.

Bytes left: The amount of data left from the transfer operation. Only applies to download transfers, since the FTP protocol does not let the server know the size of the file being uploaded in advance.

Est. time left: The estimated time remaining from the transfer operation. Only applies to download transfers, for the same reason as the previous item.

Kick: This button kicks the user out – in other words, terminates the connection.

Ban user: This button kicks and then bans the user from the FTP server. Only applies to FTP users, and not to NT users. The user's properties will show him as disabled on the server he was banned from.

Ban user IP: This option first kicks the user from the server in question, then adds an IP filtering rule to the user object that will prevent him from logging in again from the IP address in question. He will have the ability to log in from other IP addresses (depending on IP filtering setup) and the IP address will only be disabled for this user.

Ban server IP: This button kicks the user, then adds an IP filtering rule to the server object that will cause the server not to accept connections from the IP address in question at all. The user will be able to log in from other IP addresses.

Anti-hammering: information for each server is also shown, where applicable. It is in the following format:

IP address: The address the attempted connection came from.

Expires at: The time when the information will be discarded – users will be able to establish connections from the IP address at this time again.

Bad logins: Number of bad logins from the IP address.

Delete: Clicking this button will remove the anti-hammering information from the FTP server's memory, thus making the IP address available for logins, had it been locked out.

The Refresh button refreshes the contents of the screen to reflect any changes, while the Back button goes back to the main FTP settings screen.

FTP Statistics

If you click on FTP Statistics under Server Functions in the menu you can view per-server and per-user statistics, such as the last login, number of logins, bytes sent and received, etc.

The red button labeled Reset for servers and FTP users, or Delete for NT users will reset or delete statistics kept on that object.

Port Forwarding Server (RemotelyAnywhere Server Edition only)

RemotelyAnywhere Server Edition also comes with Port Forwarding Server. This allows you to forward one or more TCP or UDP ports on one computer to another so that separate networks can be bridged.

Before getting into the details of how you would configure your Port Forwarding Server (PFS) we will look at how it works. Picture the following scenario:

You have a Local Area Network (LAN), connected to the Internet with a firewall / proxy server. The computers on the LAN all have non-Internet IP addresses, and they connect to the outside world via the proxy server.

If you have RemotelyAnywhere installed on any computer on the LAN — say, the fileserver — you would be able to access it from within the LAN without any problems. However, it is not accessible from the Internet.

If you set up RemotelyAnywhere Server Edition and PFS on the firewall, so that a certain port (say, 3000) on the firewall is forwarded to the fileserver's IP address and RemotelyAnywhere port (2000 by default), accessing port 3000 on the firewall will let you access RemotelyAnywhere on the fileserver - both from within the LAN and from externally.

Port Forwarding Configuration

When you click on Port Forwarding Configuration under Server Functions in the menu you can set up the above scenario. In order to look at the interface for this feature we will look at some more possible scenarios.

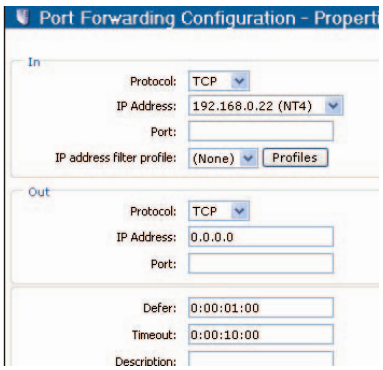
Imagine, as an example, the following scenario:

- The firewall's Internet IP address is 145.236.120.227
- The firewall's LAN IP address is 192.168.0.2
- The fileserver's LAN IP address is 192.168.0.10
- RemotelyAnywhere is installed on both computers, and is listening on port 2000.

> The IP addresses used in the foregoing are for demonstration purposes only.

What we need to do is simple: map port 3000 on the firewall computer to port 2000 on the mail server (dns name: mailserver.company.com).

Having called up the Port Forwarding Configuration screen from the menu, you can now add a new rule by clicking **Create forwarding rule**. This will present you with the following dialog box:



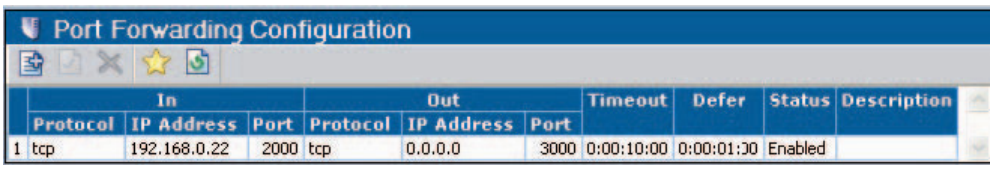
The Incoming Protocol field will be TCP. Other protocols (SSL, CSSL) will be discussed later. The Incoming IP Address can be either All available meaning that the port will be forwarded from all IP addresses of the firewall. If you want to use a single IP address instead of all assigned ones, select it here. The Incoming Port can be anything not already in use on the computer - let's assume 3000 for now.

The Outgoing Protocol will be TCP. The Outgoing IP Address will be mailserver.company.com (or the actual IP address of the host), and the Outgoing Port will be 2000.

The Defer Close and the I/O Timeout values can be left to their defaults. These will be explained later.

The Description field lets you specify a remark associated with the port forwarding item. This will be displayed on the main screen.

If you fill out the dialog and click **Add**, the item will be listed on the main PFS screen:



That's really all there is to it. Your first port forwarding item has now been configured.

Advanced Options

You can edit a port forwarding item by double clicking it, or by selecting on it and clicking on the **modify rule** button.

You can specify IP address restrictions for the item from the IP filtering drop down. This works exactly like the RemotelyAnywhere IP Address Filtering feature, only it restricts incoming connections to the corresponding port forwarding item only. For more information, please read the documentation on **Security > IP Address Filtering.**

I/O Timeout: This setting lets you specify how long the PFS will hold a connection open with no data going through it in either direction. When the amount of time specified here is reached and the connection is idle, both ends of the connection will be closed gracefully.

Defer Close: This setting lets you specify a timeout value for a special condition. When one end of the connection has been closed, but the other is still open, PFS will wait this much time for the open end of the connection to be closed. It will then close the connection itself.

Incoming and Outgoing Protocol: These fields let you specify SSL or CSSL as well as TCP. To translate SSL connections to TCP or TCP to SSL, and thus behave as an SSL proxy for applications that are not SSL-enabled, simply set one end to SSL and the other end to TCP.

There are situations when SSL encryption would be a very nice thing to have, but neither the client nor the server support it. In this case, you can use two installations of RemotelyAnywhere: one to translate the connection from TCP to SSL, the other to translate it back from SSL to TCP.

Let us suppose that you are using a laptop with a dialup account, and your email software does not support SSL. Let's also suppose that your corporate mail server does not support SSL either. If you still want to keep your email secure, you can install RemotelyAnywhere both on your laptop and on the email server, and set up a port forwarding item on both computers.

On your laptop, you would need to do the following:

1. Create a port forwarding item with the incoming IP address as 127.0.0.1 (the loopback address), the incoming port as 3110, the incoming protocol is TCP. The outgoing IP address or host name would be set to that of your email server, the outgoing port would be set to 3110, and the outgoing protocol would be SSL.

2. Change your email client's preferences so that the POP3 server is 127.0.0.1 and the port is 3110.

On the mail server, you would need to only create one port forwarding item, with the incoming IP address set to your mail server's Internet IP address, the incoming port would be 3110, and the incoming protocol would be SSL. The outgoing IP address would be the same (the mail server's Internet IP address), the outgoing port would be 110 (the standard POP3 port), and the outgoing protocol would be set to TCP.

If you performed the above three steps, starting up your email client and checking for mail would actually go through two port forwarding servers; the first one being on your own computer, encrypting all data before it's sent to the mail server. The mail server's port forwarding server would receive the encrypted data, and decrypt it before sending it on to the actual mail server software. Data flowing in the other direction would be also seamlessly encrypted and decrypted.

However, if you have two RemotelyAnywhere Port Forwarding Servers talking to each other, you could also utilize the proprietary CSSL protocol instead of using plain SSL. CSSL, which stands for Compressed SSL, would also seamlessly compress and uncompress your data as well as encrypt and decrypt it - to keep to the above example, making your mail arrive much faster over a dialup connection. (And also, to properly finish the laptop/email example, you would also have to create one additional port forwarding item on both computers for the SMTP protocol that is used to send email as opposed to receiving it. This runs on port 25 by default.)

Port Forwarding Status

If you have configured your Port Forwarding Server as in the examples above, you will be able to view the status of your Port Forwarding connections by clicking on Port Forwarding Status under Server Functions in the menu.

Active Directory

This is an Active Directory browser. It lets the user connect to and browse through the various elements in the Windows 2000 domain's active directory tree. It's usually employed as a simple system info tool.

Scheduling & Alerts

Under Scheduling & Alerts you can make use of RemotelyAnywhere's scripting capabilities, as well as set up a service to send you email alerts when certain events occur on the remote machine.

System Monitoring

This is a powerful feature of RemotelyAnywhere enabling you to monitor the system based on the performance data collected. You can also define conditions, and actions to be performed. A condition and an associated action are known as a rule.

Rules are defined in the file **MonitoringScript.txt** located in your RemotelyAnywhere directory. You can edit this file using your favorite text editor, or you can use the System Monitoring option under Scheduling & Alerts in the menu to make changes and create new rules.

A rule has the following structure:

```
<rule name> (delay)
        { <condition> { <action1> } else { <action2> } }
```

For example:

```
"Check Memory Usage" (10m)
{
        MemUsageAboveFor(70%, 20m)
        {
                SendMail("administrator@company.com",
                        "Memory usage on [MACHINE]",
                        "High memory utilization!\n"
                        "(Max: [MAX_USAGE])");
        }
        else
        {
                SendMail("administrator@company.com",
                        "Memory usage back to normal",
                        "See topic.");
        }
}
```

The above rule executes every 10 minutes (delay), and checks the condition MemUsageAboveFor. In the above scenario, if the memory utilization is above 70% for 20 minutes or more, the condition becomes true, and action1 is executed.

The action, in this case, will send an email to administrator@company.com describing what has happened. The rule will keep checking the condition every 10 minutes after the condition has become true. If it's still true, it does nothing – but if it becomes false (that is, the emergency situation is resolved) it executes action2. In that case, RemotelyAnywhere will email the administrator to let him know that the problem has been resolved.

The action can consist of several statements – they have to be separated with a semicolon. Such as:

```
MemUsageAboveFor(70%, 20m)
        {
                SendMail("administrator@company.com",
                                "Memory usage on [MACHINE]",
                                "High memory utilization!\n"
                                "(Max: [MAX_USAGE])");
                SendMessage("administrator",
                                "High memory utilization on [MACHINE]!\n"
                                "(Max: [MAX_USAGE])");
        }
```

There is one special rule that can – and should - be defined: it's called ERROR. If something goes wrong while performing actions – for example, when the user Administrator is not logged on and the above actions are executed, **SendMessage** will fail – **ERROR** is executed, allowing you to customize error-handling behavior.

The **MonitoringScript.txt** file that ships with RemotelyAnywhere defines a number of sample rules. They are all commented out – you will need to remove the comment marks (#) from the beginning of each line of a rule you'd like to use.

You will find a full list of conditions, actions and string substitutions in Appendix B.

It might seem overwhelming at first, but if you have a little bit of experience of programming in C or a similar language (escape sequences and string formatting are C-like) and study the sample MonitoringScript.txt for a little while, you will be up and running sooner than you thought.

You can enable or disable certain conditions with the dialogue that appears when you select System Monitoring

The Edit script button lets you edit the monitoring script in your browser.

Email Alerts (Vista/XP/2000/NT4 only)

When log entries matching a certain criteria are entered into any of the event logs you can have RemotelyAnywhere send you email alerts to an email address of your choice.

Email alerts will not work until you configure your SMTP server under **Preferences > Network.**

Once you've set that up, you can configure email alerts according to the following criteria:

Log: The event log to watch.
Type: Can be Error, Warning or Information. It is not necessary to specify this field.
Source: Type in the source of the message you want to be alerted on. For example, Security, Disk, etc. This field is optional.
Category: Type in the category of the message as it would appear in the event log. This field is optional.
Event: Type in the event code as it would appear in the event log. This field is optional.
Email: The email address the notifications are sent out to. You can only specify a single email address per entry, so if you want several people to receive these messages you should specify a group alias here.

Task Scheduler

This function **(Scheduling & Alerts > Task Scheduler)** differs in behavior on NT and W2K systems. On NT, it gives you a simple interface to NT's Scheduler. In order to be able to view, add and delete tasks, the Schedule service must also be running.

On W2K, it interfaces with the updated task scheduler service instead of the old, still present Scheduler. It allows you to create multiple triggers for a single task, specify different user accounts to run tasks under, and so on. It supports the entire feature set of the W2K Task Scheduler.

On the main page, you can see a list of all currently scheduled tasks. The table shows you the following:

- The ID of the task
- The command to be executed
- The time of the day the command is to be run
- The days of the week and month on which the command is scheduled to run
- Whether the command is interactive (that is, shows on the desktop)
- Whether the last run of the job ended successfully

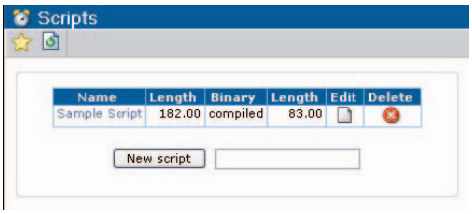
You can remove a task from the list by selecting it and clicking on the delete button in the toolbar.

You can add a new scheduled task by clicking on the Create New Task button. You can also check and modify the

attributes of your existing tasks by double clicking them or via the Change attributes button in the toolbar. These attributes are organized under three tabs, with the headings Task, Settings and Schedule.

Scripting

RemotelyAnywhere provides an extension interface in which you can create custom scripts that interact with the system, RemotelyAnywhere and the user. This is available under Scheduling & Alerts > Scripting, and this is what you'll see when you select it:



Clicking on the name of the script will execute it. The Edit command will bring up a page with the source code of the script, where you can edit and compile your program. The Delete command removes the script.

To create a new script, enter its desired name in the input field and click the New script button.

There are three kinds of scripts you can create:

1. **Interactive**
2. **Quiet**
3. **Hybrid**

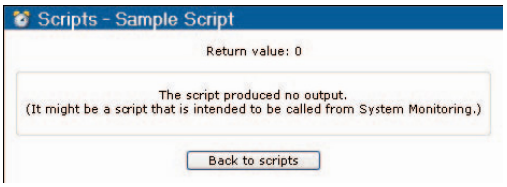
Interactive scripts display their output on HTML pages, within the RemotelyAnywhere frameset. An example for an interactive script is the File.sma script, which is installed with RA. These scripts do not have to return a value from their main function. They communicate with the user via the htmlBeginOutptut(), htmlEndOutput(), and various other html***() functions.

A Quiet script is one that is usually called from the System Monitoring script. It does not display output. A return value is required at the end of the main function.

A skeleton example for a Quiet script is:

```
#include <ra>
main ()
{
        return 0;
}
```

This script does not do anything useful. It simply returns a zero value, meaning that no problem has occurred. If you attempt to run this script from the Script menu, you will get a message similar to this:



Hybrid scripts, on the other hand, are executable interactively and also return a value at the end of their main function. An example for a hybrid script is the WatchProcess.sma file, included with RemotelyAnywhere. Hybrid scripts check the return value of the htmlBeginOutput() function, and if it's a zero value, the script is run in non-interactive mode. (That is, it is invoked from the System Monitoring script, via the Small() function call.)

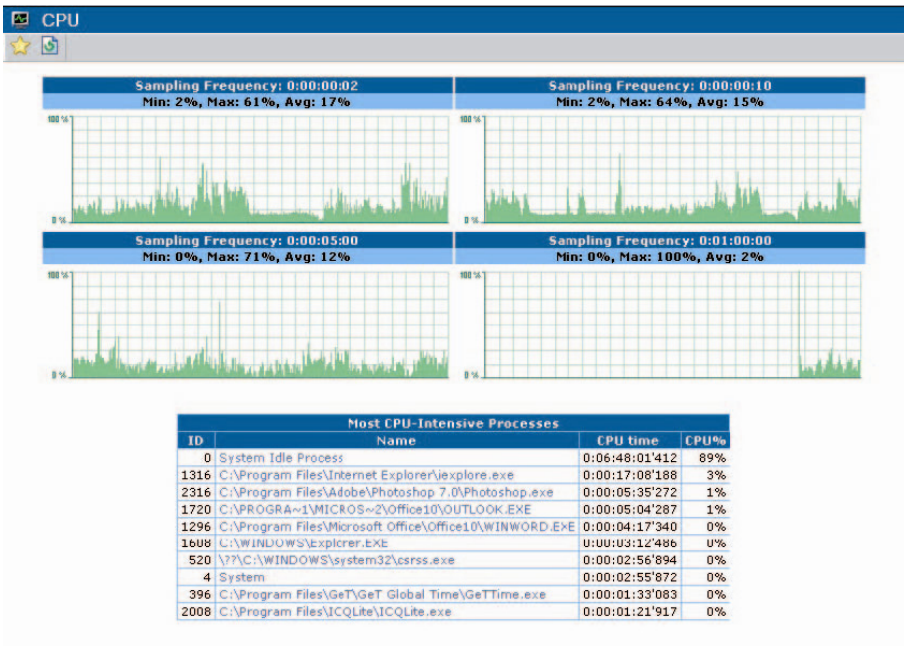
For a complete reference of the scripting language, please see Appendix B, and the Small Booklet (smalldoc.pdf), also included with RemotelyAnywhere.

If you have experience in programming in C or C++, and have a basic understanding of HTML, you will very quickly be creating your own scripts.

Performance Monitoring

The menu items under Performance Monitoring allow you access to the performance data collected by RemotelyAnywhere. Descriptions for each of the choices can be found below. When you open this branch of the menu tree you'll notice that all the items are just data pages. They can only be configured under **Preferences > System Monitoring.**

CPU Load



This option takes you to a page with a number of graphs and lists. The graphs show CPU utilization with various sampling rates. Please note that RemotelyAnywhere needs time to gather performance data for these graphs. If you have just installed the software, it is likely that only the left-hand side of the first graph will show you meaningful information. If you have multiple CPUs in your computer, you will see separate graphs for each one, as well as a set of graphs showing you the total CPU load.

The sampling rate for the first graph is 2 seconds, so the graph spans less than an hour. This is useful to see what's happening right now on the machine. If you move your mouse over a line in one of the graphs, the tooltip that pops up tells you exactly when the sample was taken.

The list at the bottom shows the processes that take up most of the processor time. This list is weighted, so younger processes that take up a lot of processing time come closer to the top. (The figure is: PROCESSOR_SECONDS/PROCESS_AGE_SECONDS). So, if you see a sudden spike on the first graph you can

check the second list and immediately find out which process is eating up processor time.

Clicking on an item in the ID column will display the relevant data on that process, organized under six separate tabs (General, Threads, Services hosted, DLLs, Open Files, and Registry Keys In Use).

Memory Load

This will present you with four graphs similar to those on the CPU Load page. These display the memory utilization on the machine.

Disk Space

Graphs displaying the disk space utilization per logical disk are available under this menu item.

Drive & Partition Info (Vista/XP/2000/NT4 only)

This page displays all physical drives in the remote computer and their partition tables. This data is organized onto two separate tabs for Physical Drives and Partitions, and Logical Drives.

Open TCP/IP Ports (Vista/XP/2000/NT4 only)

This will present you with a listing of all open IP endpoints on the computer. You can specify whether you'd like to see the ports that are listening for connections, ports that have been connected to another computer, and ports in various stages of being connected and disconnected. You can also elect to have RemotelyAnywhere resolve IP addresses appearing in the list of hostnames - please note that this can take a considerable amount of time.

Network

Under Network you can find feedback on your network traffic. The four graphs offer different timelines of 2 seconds, 10 seconds, 5 minutes, and 1 hour on your inbound or outbound traffic.

You can set the Maximum Inbound Bandwidth according to the appropriate kilobits per second in order to be sure of accurate results.

PCI Information

If you click on PCI Information you can view all hardware connected to the PCI bus or buses in the system.

Open Files

This will show a listing of all files currently open on the remote computer, along with the names of the processes using them. The processes list is clickable, so you can view data on the processes, and if necessary, kill them.

Registry Keys in Use (Vista/XP/2000/NT4 only)

Under Registry Keys in Use you can view a list of all registry keys currently open on the remote computer. As with open files, you can also see the names of the processes that use them. The processes list is clickable, so you can

view data on the processes, and if necessary, kill them.

DLLs in Use

Here you can view a listing of all currently loaded dynamic link libraries and the processes that use them.

RemotelyAnywhere Connections

Selecting this option will display all current connections currently being served by RemotelyAnywhere. It will display the IP address and host name of the remote computer, the type of connection and the name of the Windows NT user associated with the connection. The connection type can be one of the following:

(Browser) HTTP: A typical browser connection requesting a page.

Remote Control: A Java remote control client.

Upload Status Viewer: A Java applet displaying the progress of a File Manager upload.

Performance Viewer: The Java applet above the menu, displaying CPU and memory utilization.

Telnet/SSH Connections

Selecting this option will display all current Telnet/SSH connections currently being served by RemotelyAnywhere. It will display the IP address and host name of the remote computer, the type of connection and the name of the Windows NT user associated with the connection.

Installed Applications

Under Installed Applications you will find a useful list of applications installed on the remote machine. This list is populated from Add or Remove Programs on the remote machine's Control Panel.

The data is for information purposes only, but in addition to the program name and version you will be able to see the Publisher, Installation Directory and frequency of usage, if this information is available. If you roll over a listed application you may also be able to see other data such as estimated size, the installation source, registration data, and the time and date it was last used.

Motherboard Status

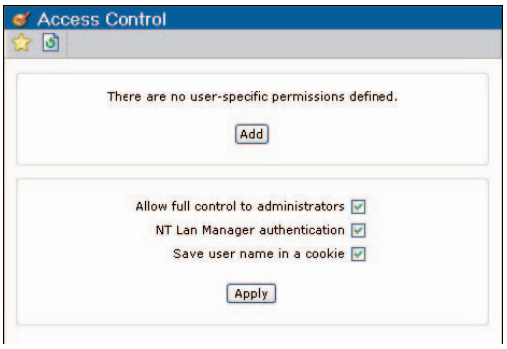
This feature relies on a 3rd party free product created by Alex van Kaam called Motherboard Monitor. If you have this software installed on your system, RemotelyAnywhere can extract information from it and display it here. MBM can provide you with the following information: chassis and CPU temperatures, fan speeds and voltages. MBM can be found at: http://mbm.livewiredev.com

Security

The menu items under Security allow you access to RemotelyAnywhere's numerous enhanced security features.

Access Control

Under **Security > Access Control** you can control who has access to RemotelyAnywhere. This is slightly different on Windows 9x and Windows NT, due to lack of a user database on the Windows 9x family of operating systems. We'll cover Windows NT first.



Before getting into the details of setting up users here we'll look at the lower part of the Access control page. Here you can enable or disable the following features:

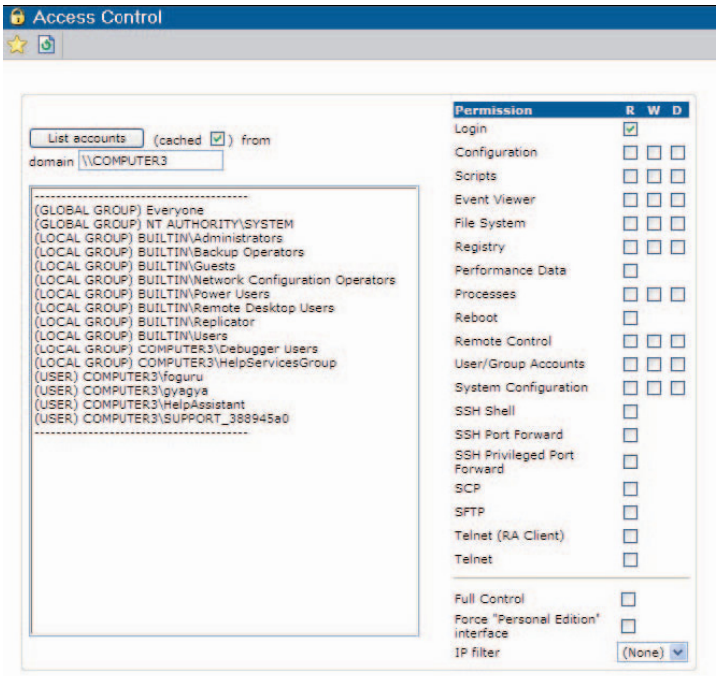
Allow full control to administrators: This is enabled by default. It adds Full Control permission to all administrators of the computer. If you turn it off, only users explicitly granted permission to use RemotelyAnywhere will have access.

NT LAN Manager Authentication: Enable/Disable NTLM authentication. For those of you concerned about security, RemotelyAnywhere supports the Windows NT Challenge/Response type authentication. You must use Internet Explorer to take advantage of this feature. Netscape will always use the default authentication method, which means that passwords travel in Base64-encoded clear text over the network. You need not worry about exposing your password to eavesdroppers if you are using HTTPS to secure all communications between your browser and RemotelyAnywhere.

Save user name in a cookie: Finally, you can configure RemotelyAnywhere to remember your user name in a cookie.

The upper portion of this dialog box lists users already granted access to RemotelyAnywhere. The Add button lets you specify a Windows NT user or group, and the access mask you wish to assign. The red Remove button next to each entry in the list will remove that user or group from the access list.

Here is the dialog box showing you the options available for an entry in the permission list:



You can select individual permissions, or specify Full Control. You can also restrict the user to an IP address or a network by entering the appropriate parameters in the fields below. To restrict the user to a single IP address, enter it in the IP Address field, and leave Subnet Mask blank. To specify access from a network, enter the network address in the IP Address field, and enter the subnet mask in the Subnet Mask field.

The **R**, **W** and **D** columns allow you to specify powers to read only (R), write (W), or delete content (D). All three on Remote Control, for example, will allow user access to a remote machine without asking for permission from the interactive user on the host. Just uncheck **D** to force this dialog to appear before accessing the remote machine.

Login: Anyone with any sort of access to RemotelyAnywhere is implicitly granted Login access. This allows for looking at the Info page, reading the Help file, chatting with the user in front of the computer, and logging out.

Configuration: Users with access to the Configuration module can re-configure RemotelyAnywhere. This also

grants users access to modifying RemotelyAnywhere permissions; keep this in mind!

Scripts: Users can execute, create, change or delete scripts.

Event Viewer: Allows the use of the Event Viewer module.

File System: Allows access to and the use of the file system on the remote machine.

Registry: Allows for editing and compacting the registry.

Performance Data: Ability to view performance and system information data.

Processes: Allows access to the Process List, and adds the ability to terminate processes and/or change their priorities.

Reboot: Allows rebooting the computer and restarting the RemotelyAnywhere service.

Remote Control: Allows use of both the screenshot-based and the Java-based Remote Control module.

User / Group Accounts: Allows the use of the User Manager module.

System Configuration: Access to setting the time, using the Shared Resources administrative page and changing virtual memory settings under the Computer Settings menu option.

SSH Shell: Allows access to a command prompt on the host computer via the SSH protocol.

SSH Port Forward: This option grants the user the right to use SSH port forwarding.

SSH Privileged Port Forward: This option grants the user the right to use SSH privileged port forwarding.

SCP: This option grants the user the right to use SCP.

SFTP: Allows the user access to the filesystem of the host computer via the SFTP (Secure File Transfer Protocol, an extension of SSH) protocol.

Telnet (RA Client): This option allows the user to use the secured telnet client found in the browser under Computer Management > Command Prompt.

Telnet: Allows access to the machine via Telnet - either using the built-in telnet client or any standalone terminal emulator.

Full Control: Adds all possible permissions to a user. It is recommended to have at least one account that has Full Control capabilities.

IP Filter: This assign an IP filter profile to the user, and specifies which IP addresses from which he or she can or cannot connect.

Special care needs to be taken with a few of the above options. Users with access to Configuration and Registry Editor can also access and change the RemotelyAnywhere configuration data, including permissions. However,

the Registry Editor option can be considered safe, since the administrator can change permissions on the HKLM\Software\RemotelyAnywhere key and protect it from unwanted access. Users who can Create/Edit Scripts can also create programs in the Small language that run on the remote computer. These scripts will be run under the account of the person starting the script from the Scripts menu – except when a Small program is called from the system monitoring script. In this case, the program is run under the LocalSystem account.

With the exception of the Reboot, Remote Control and Processes, Windows NT access restrictions apply. For example, you can grant someone access to the File Manager, but they will only be able to access files and directories their Windows NT account has permissions to. The same goes for the Registry Editor, User Manager, etc.

The above exception for Reboot, Remote Control and Processes is made to provide you maximum control over your system, and RemotelyAnywhere uses the all-powerful LocalSystem account to perform the above tasks. For example, not even an Administrator has sufficient rights to terminate a service process - but with RemotelyAnywhere performing this action under the LocalSystem account, any process can be terminated. Remote Control is another exception. When you are remotely controlling the system with RemotelyAnywhere, you have access to the mouse and the keyboard of the system. If nobody is logged on interactively, you will need to use the NT Logon dialog to gain access to the desktop, typing in a username or password, possibly different than the one you are accessing RemotelyAnywhere with. If there is a user logged on to the host computer, you will be working under his account.

Access rights are cumulative. That is, if Group A has access to the Event Viewer, and Group B has access to the File Manager, a user who is a member of both groups will have access to both modules.

If the machine is a domain controller, the user accounts and groups that appear are listed from its domain. If the computer is not a domain controller, local users and groups are displayed. You can specify where to list accounts from by typing the name of the domain or the computer in the input field and clicking the List accounts button.

You can also restrict a certain user to an IP address or an IP address range. Please remember that access rights are cumulative: if Group X has full access to RemotelyAnywhere and is not bound to an IP address and User Z is a member of that group, he will always have full access, even if you bind him to a specific IP address or network. To allow a user or group access from two or more IP addresses or networks, simply grant them the same permissions several times, but with different IP restrictions.

Access rights are stored in the registry value HKEY_LOCAL_MACHINE/Software/RemotelyAnywhere/Permissions in binary form. This data is basically a listing of the Security Identifiers of the groups or users, the access mask associated with them, the network they might be restricted to, and a CRC value. By default, any data under the HKEY_LOCAL_MACHINE/Software key

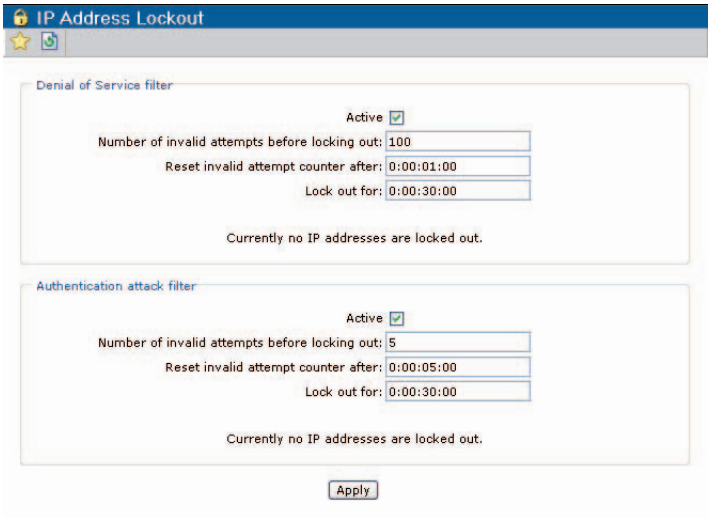
can only be changed by administrators or the LocalSystem account. Windows NT reserves the latter for services and the operating system itself.

IP Address Lockout

With RemotelyAnywhere's IP Address Lockout feature you can detect and temporarily lock out potential intruders.

This security precaution allows you to configure two specific types of filter. These are called the Denial of Service Filter and the Authentication Attack Filter. The first is a precaution against unwanted intruders who slow your remote machine to a halt by continuously requesting the same service. The second locks out those who persistently try to get past your log-in screen without authorization.

The configuration for each is identical, although the default values differ due to the differences in the kind of attack they are designed to prevent.



Active: By ticking this box you will enable this feature. This can be useful if your server is exposed to the Internet. IP Lockout will prevent people from gaining access to the administrator username and password using brute-force methods, or from tying up your services through relentless requests.

Number of invalid attempts before locking out: Specify the number of login attempts before a lockout occurs.

Reset invalid attempt counter after: After the amount of time specified in this box elapses, the invalid attempt count of the offending IP address will be reset to zero.

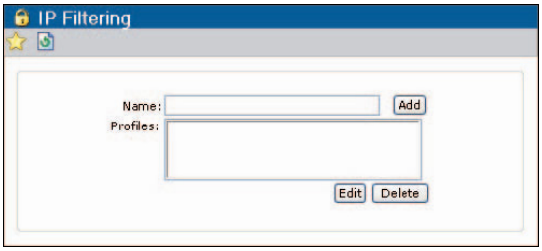
Lock out for: If there were a number of bad login attempts from the same IP address, as specified in the second

field, within the time period specified in the reset count field, all attempted connections from the offending IP address will be rejected for the amount of time given here.

Bad login attempts and lockouts are logged in the RemotelyAnywhere.log file if you have logging enabled.

IP Filtering

With RemotelyAnywhere's IP address filtering feature you can specify exactly which computers are allowed to access RemotelyAnywhere on your system.



The above simple interface lets you maintain IP address restrictions. If the Current IP Address Filters list is empty, then filtering is disabled.

The Up, Remove and Down buttons let you manage already entered filters. Select one item in the list, and move it up or down with the appropriate buttons, or remove it altogether.

The New Item fields let you specify a new filtering item. You can enter the following:

1. A single IP address
2. An IP address with a subnet mask, essentially granting or denying access for a whole network.
3. An IP address with wildcards and no subnet mask. Accepted wildcards are an asterisk (*) that matches any number of characters, or a question mark (?), that matches a single character only.

The Allow and Deny drop down lets you specify whether you want to allow or deny access to the IP address or addresses entered.

Whenever a new connection is established to RemotelyAnywhere, the remote IP address is checked against the filter or filters in the list, and access is granted or denied accordingly. The IP filters that you set up here apply to every connection received by RemotelyAnywhere, except for those aimed at the FTP or Port Forwarding Server. To specify IP address restrictions specific to these modules you will need to use their specific IP filtering options (see Section Guide - Server Functions).

How IP Filtering Works

When an IP address is checked against a list, RemotelyAnywhere goes from the first element of the list to the last, comparing the IP address against the item. If the item is a single IP address, it only matches the remote IP if they are equal. If the item is an IP address with a subnet mask, a logical AND operation is performed on the subnet mask and the remote IP address, and the result is checked against the item's network address to see if the remote IP address is in fact on the network. If the item is a wildcard, the remote IP address is converted to its dotted textual representation and the two strings are compared.

When a match is found, RemotelyAnywhere checks if it should allow or deny the connection, based on the allow/deny flag belonging to it. This result is then used to decide whether to let the connection proceed.

If no match is found, then the connection is allowed. If you would like all connections to be denied by default, except for those in the list, enter a DENY:* line as the last item on the list.

Examples:

1. Allow connections from IP address 215.43.21.12 and the network 192.168.0.0, and deny all other connections:

   ALLOW:215.43.21.12
   ALLOW:192.168.0.0 (255.255.0.0) –OR- ALLOW:192.168.*
   DENY:*

2. Allow connections from IP address 215.43.21.12 and the network 192.168.0.0, but not from the address 192.168.0.12, and deny everything else:

   ALLOW:215.43.21.12
   DENY:192.168.0.12
   ALLOW:192.168.0.0 (255.255.0.0) –OR- ALLOW:192.168.*
   DENY:*

Please note that denying the connection from 192.168.0.12 comes before allowing connections to the 192.168.0.0 network. This is because if RemotelyAnywhere was to find the ALLOW item first, it would let IP address 192.168.0.12 through, since it matches the condition. To prevent this, we make sure that the address 192.168.0.12 is checked before the network to which it belongs.

3. Allow all connections, except those coming from 192.168.0.12:

   DENY:192.168.0.12

4. Deny all connections from the network 192.168.0.0 except for the subnet 192.168.12.0, and allow all other connections:

   ALLOW:192.168.12.0 (255.255.255.0) –OR- ALLOW:192.168.12.*
   DENY:192.168.0.0 (255.255.0.0) –OR- DENY:192.168.*

Yet again, ordering is crucial.

It is not possible for you to lock yourself out by accident when setting up IP address restrictions from afar, i.e. you can't enter a DENY:* clause into an empty list.

RemotelyAnywhere Logs

In order to view the RemotelyAnywhere log files, this is where you should look.

The active log file is at the bottom of the list and is named RemotelyAnywhere.log. Older logs are stored with the naming convention RAYYYYMMDD.log. For example, the RemotelyAnywhere log file for June 1st 2003 would be called RA20030601.log.

You can enable or disable logging to text files as you will, but RemotelyAnywhere will always log the following events to the Windows NT/2000 Application Log:

1. Service Start/Stop
2. Login/Logout
3. Remote Control Start/Stop
4. Telnet/SSH Login/Logout

The Application Log is used because of security considerations.

In addition, service start and stop events are always written to the RemotelyAnywhere.log file, no matter whether logging is enabled or disabled. You can modify the settings for these logs under Preferences > Log Settings.

SSL Setup

If you set up SSL support for RemotelyAnywhere all traffic between the host and the remote computer will be encrypted using industry-strength 128-bit ciphers, protecting your passwords and data. You can do this fairly easily by going to Security and clicking on SSL Setup.

RemotelyAnywhere can detect and use any SSL certificates already installed in Windows on your machine, as long as they have an exportable private key.

You will be given a choice whether you'd like to use one of your already installed certificates or create a new self-signed certificate.

To select a previously installed certificate select -- Look in Certificate Services -- and then click on Continue.

You will be displayed a list of Certificate Services found in your domain. Select the one from which you wish to request your RemotelyAnywhere server certificate.

If you'd prefer to create your own self-signed certificate, it can be done in four easy steps:

1. Set up your Certificate Authority (CA). This step will create a CA certificate, valid for ten years, and self-sign it. Simply fill out the form at the bottom of the page specifying your country code, your organization and your name. Some default values are provided here from your computer's registry. When you've finished, click on the Create CA button. This will create the CA. Click on the Continue button at the bottom of the page when you're ready for the next step.
2. Create the server certificate. Simply fill out the form at the bottom and click on Create Certificate to proceed. RemotelyAnywhere will generate a certificate request, and sign it with the Certificate Authority you created in the previous step. The certificate created this way will be valid for ten years. Click Continue on the next screen.
3. (optional) Install the CA certificate in your browser. This will suppress the message you'd otherwise get about the unknown Certificate Authority every time you make a secure connection to RemotelyAnywhere. Click on the button and follow the instructions on screen.
4. Restart RemotelyAnywhere so that it can load the newly created server certificate. You can do this from the Control Panel or the console by typing net stop RemotelyAnywhere and net start RemotelyAnywhere.

That's it. You are now ready to make a secure connection to RemotelyAnywhere. Simply use a URL in the form of https://my.machine.here:2000.

Note: you can use the same CA certificate on several machines, but you can't use the same server certificate in more than one place. If you want to use one CA certificate on a network of NT machines, simply perform step one on the first machine, then copy the files CACert.pem, CAKey.pem and CACert.der in the RemotelyAnywhere directory to the other machines. You can then continue SSL setup from step two on all other boxes. You only have to perform step three once in this case.

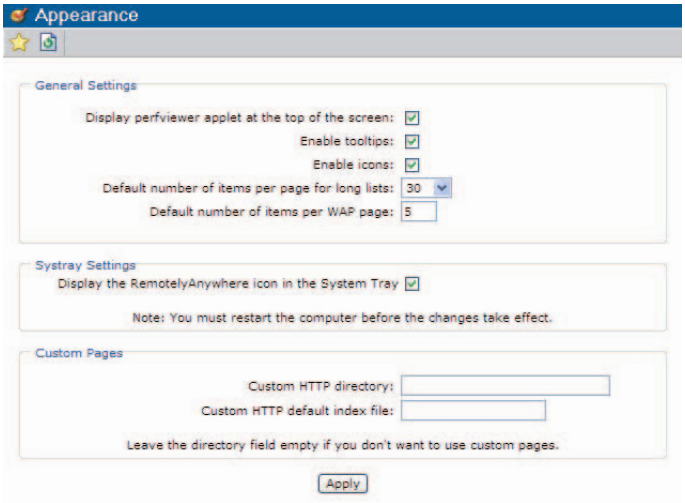
The SSL certificates generated here are used for accessing the HTML-based administration module via HTTPS, and are also used by all virtual FTP servers to secure connections if using a suitable client.

Preferences

RemotelyAnywhere is a highly configurable tool, meaning that you can change its settings to suit your individual remote administration needs and desires. When you click on Preferences in the menu a number of additional options become available for configuring the various sections of RemotelyAnywhere outlined in previous sections of this manual. In Version 4 and earlier releases of RemotelyAnywhere this option was called Configuration.

Appearance

If you select Appearance under Preferences you can tailor the look of RemotelyAnywhere to your liking.



General Settings

Display perfviewer applet at the top of the screen: Enable/Disable the Java Applet showing the current processor and memory utilization in the top frame.

Enable Tooltips: If you no long wish to display the tooltips displayed by RemotelyAnywhere, uncheck the box.

Enable Icons: You can turn off most of the icons displayed on the HTML pages.

Default number of items per page for long lists: The number of records displayed per page on those where there are long lists (such as eventlogs).

Default number of items per WAP page: Most of the WAP devices out there have very small screens and limited memory. Also, some gateways might enforce size restrictions on the WML documents they compile for their devices. This configuration setting lets you specify the number of records to appear per WAP screen, where applicable. Such screens belong to the Processes, Services, and Drivers menu options.

Systray Settings

Under **Preferences > Systray Settings** you can enable and disable the System Tray icons.

Display the RemotelyAnywhere icon in the System Tray: If you do not want the RemotelyAnywhere icon to be displayed in the System Tray, you can disable it here. Clicking on this icon gives you access to a wealth of extra information, including a log of recent events and detailed performance data graphs. This is detailed in the User Interface chapter of this manual.

Custom Pages

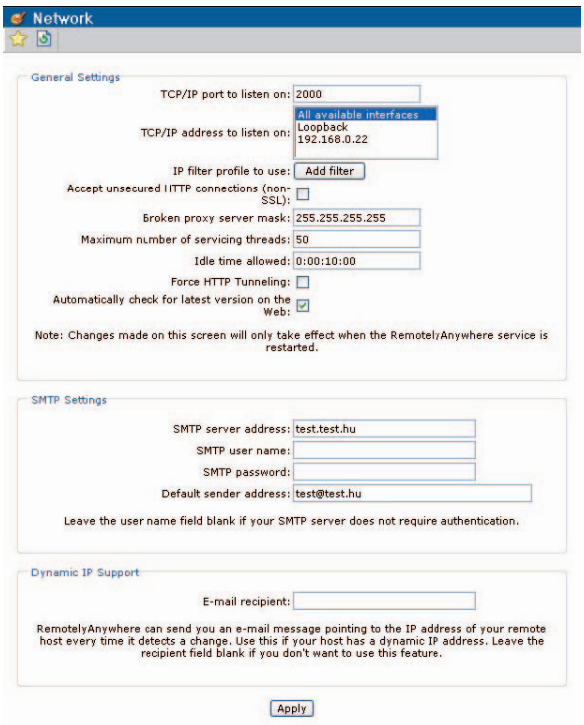
RemotelyAnywhere is able to act as a simple HTTP daemon and serve files from the computer to the Web. You can customize the HTTP daemon's behavior in the Appearance submenu under Preferences.

If you specify the root directory for the HTTP daemon, and the default index file then when you select Custom Pages (at the bottom of the menu) it will display the default index file from the web root specified.

Simply leave the directory field empty if you don't want to use custom pages.

Network

Under **Preferences > Network** you can configure your RemotelyAnywhere connection settings, your SMTP settings, and even Dynamic IP Support.



General Settings

The General Settings dialog allows you to change various connection and data transport related options.

TCP/IP port to listen on: Specify the port you want RemotelyAnywhere to use. This takes effect when the service is restarted.

IP Address to listen on: Specify the IP address you want RemotelyAnywhere to use for incoming connections. Your machine can have several IP addresses assigned to it, and RemotelyAnywhere can listen on all of those addresses or just the one you specify here. This takes effect when the service is restarted.

IP filter: profile to use Here you can select from a drop down menu of specified IP addresses. You will first need to set this up under Security > IP Filtering

Accept unsecured HTTP connections (non-SSL): If this box is unchecked and SSL transport has been set up (Security > SSL Setup) then only HTTPS connections will be allowed.

Broken proxy server mask: This is a rather obscure name for a setting provided to work around a rather obscure problem.

Some proxy servers request pages from web servers using several IP addresses. This can cause RemotelyAnywhere to bounce you back to the login page after you click the Login button. If you are not affected by this problem, you should not change this setting. However, if you experience this problem, please read the following section carefully.

When you log in, your browser is assigned a session identifier in a cookie. For security reasons, this cookie is only valid when sent from the IP address from which the login originated. Were it not so, an eavesdropping attacker would be able to copy your cookie and gain access to all RemotelyAnywhere resources to which you have access.

Some proxy servers use several IP addresses when requesting data from a remote computer. If this is the case with your proxy server, RemotelyAnywhere sees the original IP address and session identifier as valid, but requests originating from other IP addresses (even if accompanied by a valid cookie) are replied to with the login page. The login page breaks out of frames, and displays itself in your browser - and you are prompted to log in again. A possible workaround is to keep logging in as many times as necessary - most proxy servers only use a few - maybe half a dozen - IP addresses. Once all the IP addresses are logged in, you will no longer be bounced to the login page.

Since version 3.2, RemotelyAnywhere has had a setting called Proxy Problem Fixer.

This is essentially a mask that can be applied to IP addresses. Suppose your proxy server uses the following IP addresses to request pages from servers:

192.168.0.33, 192.168.0.34, 192.168.0.35, 192.168.0.36, 192.168.0.37, 192.168.0.38

In this scenario, if you look at the IP addresses in binary form, you can see that only the last three bits are different:

11000000.10101000.00000000.00100001
11000000.10101000.00000000.00100010
11000000.10101000.00000000.00100011
11000000.10101000.00000000.00100100
11000000.10101000.00000000.00100101
11000000.10101000.00000000.00100110

This means that the largest number that can be represented on three bits (111 binary = 7 decimal) has to be masked from the IP addresses when checking them against each other to verify the validity of the session

identifier cookie.

RemotelyAnywhere provides a subnet mask-like setting for this purpose. By default, it is set to 255.255.255.255 - this means that no bits are masked off. Given the above scenario, we need to mask off the three least significant bits, thus we subtract 7 (binary form: 111) from 255.255.255.255, which leaves us with 255.255.255.248. By entering this value in the Proxy Problem Fixer field, we are telling RemotelyAnywhere to ignore the last three bits.

This is a rather tedious way of getting around the problem, but short of reconfiguring the proxy server to use only one IP address, there is no easier solution. The latter is the recommended solution, since allowing several IP addresses to share the same session identifier can be a security risk. It is not really significant when you only mask off a few (three or four) bits, but if you need to decrease more and more significant bits of the IP addresses, you are putting yourself in a risky situation.

The risk is decreased significantly due to the fact that RemotelyAnywhere now uses HTTPS rather than HTTP by default meaning that the cookie is protected by SSL.

Maximum number of servicing threads: Here you can specify the maximum number of threads RemotelyAnywhere can spawn to service client connections.

Idle time allowed: Here you can specify the idle time allowed on a connection before the user is automatically logged out.

Stalled transfer timeout: Here you can specifiy the time before a stalled transfer times out.

Force HTTP Tunneling: HTTP tunneling basically allows the applets to communicate to the RemotelyAnywhere installation from behind proxy servers by issuing HTTP requests to RemotelyAnywhere.

This option has two advantages and one drawback:

- If you connect to the remote computer via HTTPS, Remote Control, Telnet, and Chat will be tunneled through HTTPS - and SSL is much more secure than the built-in encryption used by these modules when a direct socket connection is established.
- If you can not establish a direct connection to the remote computer (because of, say, a proxy server) you will not have to wait for the direct connection attempt to time out, RemotelyAnywhere will immediately try to connect via the HTTP tunnel.
- The drawback is that you will definitely notice a performance decrease when using these modules with HTTP tunneling, since tunneling requires the data to be packed into HTTP packets and usually each packet will need to establish its own connection to RemotelyAnywhere.

Automatically check for latest version on the Web When enabled, RemotelyAnywhere will attempt to connect to

http://www.remotelyanywhere.com every 24 hours to see if there is a newer version of the software available. If there is, it will notify you via the News panel on the About RemotelyAnywhere tab of the home page, as well as place an entry in the RemotelyAnywhere.log file. When RemotelyAnywhere connects to RemotelyAnywhere.com, the following information is recorded on the server:

- The version of RemotelyAnywhere making the request
- The version and family of the operating system RemotelyAnywhere is running on
- The language of the operating system
- Whether the instance of RemotelyAnywhere making the request is a trial or a licensed copy

This information is recorded for statistical purposes, to help 3am Laboratories PL better serve its customers. If you do not wish to provide this information to us, please disable this option.

SMTP Settings

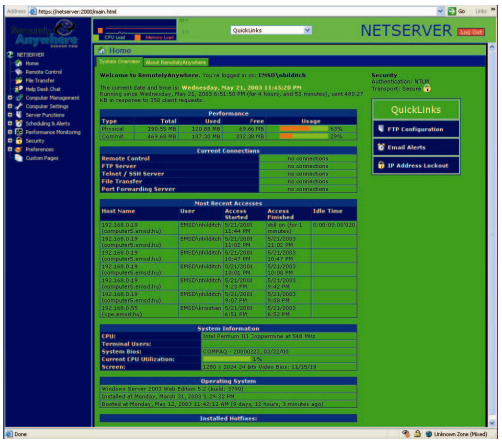
If you want to configure RemotelyAnywhere to send you e-mail alerts you need to enter your SMTP settings here.

Dynamic IP Support

RemotelyAnywhere can send you an email message pointing to the IP address of your remote host every time it starts up. Use this if your host has a dynamic IP address. Leave the recipient field blank if you don't want to use this feature.

Colors

Under **Preferences > Colors** you can modify the colors used by RemotelyAnywhere.



This is done using the standard hexadecimal code used by HTML. Simply enter the '#' symbol followed by the appropriate six-digit code and click Apply to see the change. For example, the pale blue color used for

backgrounds in the default color settings for RemotelyAnywhere is #8abdf0.

Also available is the ability to select predefined color schemes. Just select from the options in the drop down menu at the bottom of the screen and click Apply. With this option, you can even revert to the colors used for earlier releases of RemotelyAnywhere.

You can restore the default colors by clicking Restore at the bottom of the page.

Log Settings

RemotelyAnywhere's log settings are fully configurable. In order to view the logs themselves you would go to Security > RemotelyAnywhere Logs. Here, in the Preferences section you can modify the general settings for RemotelyAnywhere and the Syslog settings.

General Settings

Keep log files for this many days At midnight RemotelyAnywhere rotates its log files and deletes old, unneeded ones. The value you enter here determines how old log files can grow before they are deleted. If you set this to zero, the files will never be deleted, unless you do it manually.

Directory for log files You can also specify the directory for storing these log files. If you leave this blank, they will be stored in RemotelyAnywhere's installation folder, by default.

Send log events to ODBC data source Now that you can specify a predefined ODBC data source within RemotelyAnywhere you can also specify a data source for storing log events. See the ODBC messages option under Preferences for more information on this feature.

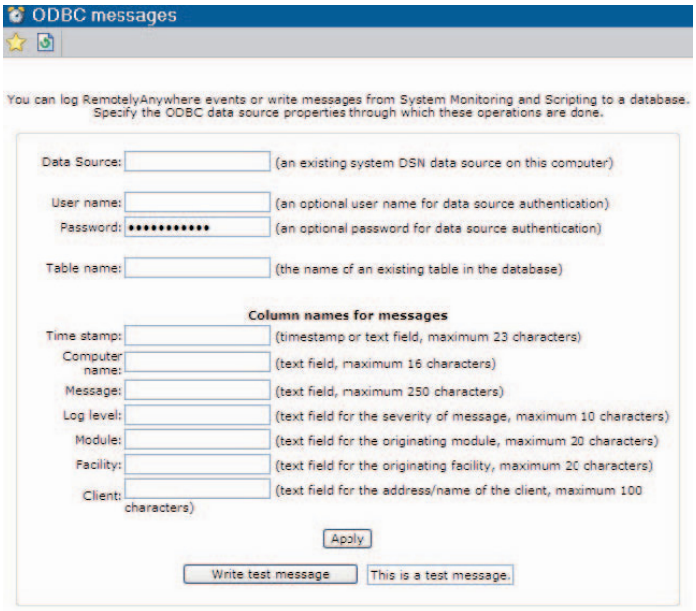
Syslog Settings

With RemotelyAnywhere version 5 you can also modify the syslog settings. Here you can specify the syslog hostname or IP address, transport protocol (UDP or TCP), syslog port numbers for UDP and TCP, as well as the facility code to report.

Click **Apply** to update your settings.

ODBC Messages

The ODBC messages feature under Scheduling & Alerts allows you to write messages from System Monitoring and Scripting to a database. By filling in the fields shown on the screen below you can specify the ODBC data source properties through which these operations are done.



Data Source Here you can enter a predefined data source on the remote host. This can be set up via that machine's Control Panel, under Administrative Tools > Data Sources (ODBC). This can be any database type: Oracle, SQL Server, Microsoft Access, or Excel.

User name & Password You need to enter the user name (including domain) and password in order to access the data source, as RemotelyAnywhere cannot imitate your login to the database.

Table Name Enter the table in which the messages are to be stored.

You can also specify the column names for the messages to be written to the specified database. The message, computer name and time stamp fields are all required.

A machine datasource must already be set up, and should contain a table with at least three fields. Specify the name of the datasource, an optional username and password, and the name of the table that will be used to hold the data. Then enter the names of the fields that will hold the timestamp, the computer name (max. 16 characters), the message itself (max. 250 characters) and other parameters.

Click Apply for these settings to take effect. You can also write a test message to correct that you have configured

ODBC messages correctly.

For more information about the kind of data that RemotelyAnywhere can collect, please see the relevant sections under **Scheduling & Alerts > System Monitoring.**

License

Under Preferences > License you can view your current license, enter updated licenses, or request an evaluation license. Simply paste the license you received when you purchased or updated your RemotelyAnywhere license into the input field, and click the Apply button. See the Getting Stared chapter for more information about activating RemotelyAnywhere after installation and requesting a trial.

The license file that you must copy without making ANY modifications looks something like this:

-----BEGIN LICENSE-----
PRODUCT RemotelyAnywhere
PRODUCTTYPE Workstation Edition
VALIDFORVERSION 6
EXPIRES 2006-06-08
LICENSETYPE COUNTED
LICENSECOUNT 1
LICENSEETYPE Corporate
LICENSEE Your Company Name Ltd
ISSUER 3am Laboratories PL
ISSUERID 1060-4b81-0781-f51c
ISSUEDATE 2005-02-22
ISSUEREASON PURCHASE
LICENSEID 52af-38f3-126e-0658
-----END LICENSE-----
-----BEGIN PKCS7-----
MIHbBgkqhkiG9w0BBwKggc0wgcoCAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEH
dG9yaWVzIFBMMRQwEgYDVQQDEwtNYXJ0b24gQW5rYQIBADAJBgUrDgMCGgUAMA0G
ATGBqjCBpwIBATBGMEExCzAJBgNVBAYTAkhVMRwwGgYDVQQKExMzYW0gTGFib3Jh
CSqGSIb3DQEBAQUABEBtenZrjzT4rXX41iYZgJ1UaONyL72nc/KEnfoM4+zHEfBk4A
sG7E6+FOa1uLSryMu4bLPj+segZZ03/GuTXjlN8l
-----END PKCS7-----

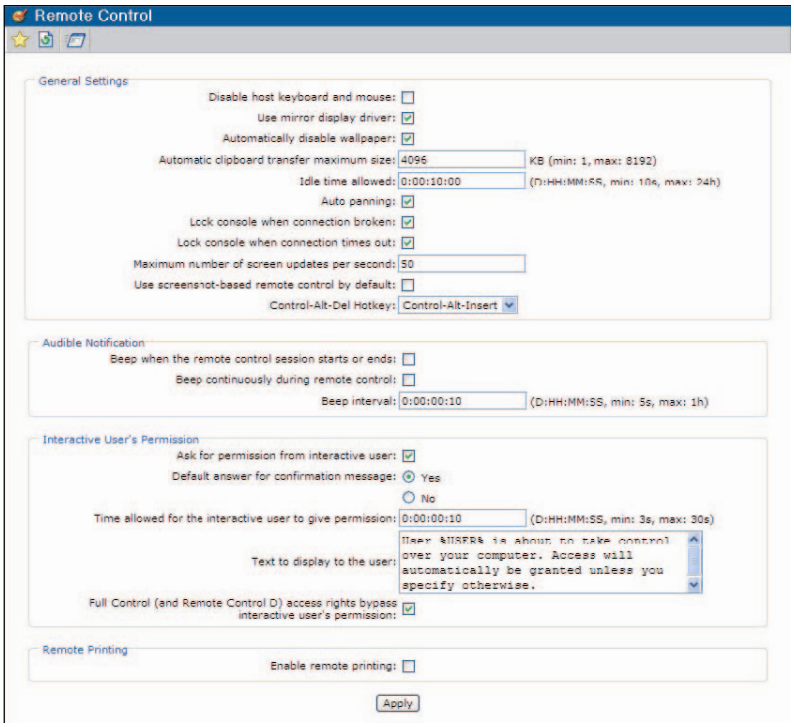
You must cut and paste everything from BEGIN LICENSE to END PKCS7 when you are prompted.

The license file contains two distinct parts. The first part is the actual license and is in plain text format. This is indicated by the BEGIN LICENSE and END LICENSE lines. The second part is the digital signature which assures the integrity of the license text. This is contained between the lines BEGIN PKCS7 and END PKCS7.

Remote Control

Under **Preferences > Remote Control** you can view and modify a number of options available during realtime remote control sessions. This includes the general settings, audible notification, interactive user permissions, and the remote printing feature, as you can see on the next page.

General Settings



Disable host keyboard and mouse: By disabling the host keyboard and mouse you can prevent the person sitting in front of the machine from using their mouse or keyboard while a remote control session is in progress.

Use mirror display driver: RemotelyAnywhere provides a mirror display driver on the W2K/XP platforms. This display driver provides a faster and less CPU-intensive remote control session. Should you have any compatibility problems, you can turn off the use of this driver by disabling this option.

Automatically disable wallpaper: By default the wallpaper (or background desktop image) on the host computer is disabled when a remote control session is started. If, for some reason, you need to be able to see this, uncheck this box.

Automatic clipboard transfer maximum size: RemotelyAnywhere version 5 features advanced remote clipboard capabilities. Its usage is outlined earlier in this manual. Under preferences you can specify the maximum number of kilobytes to be transferred between machines. The default maximum is 1024kb, but bear in mind that transferring significantly larger amounts may cause problems.

Idle time allowed: If the remote control client is inactive for the amount of time specified here, it will automatically be disconnected.

Auto panning: If the host computer's display area is larger than that which the remote control client can display only a part of the screen is shown and you can use scrollbars to view the required area of the remote display. With this option enabled, the screen is automatically scrolled for you when the mouse nears the edge of the current display area.

Lock console when connection broken: With this option enabled RemotelyAnywhere will lock the console to protect your work if, due to a network error, the Java remote control client loses its connection to the server.

Lock console when connection times out: With this option enabled RemotelyAnywhere will lock the console to protect your work if your connection times out.

Maximum number of screen updates per second: Here you can specify the number of times the screen is updated every second.

Use screenshot-based remote control by default: Here you can enable screenshot-based remote control, which menas that when you click on Remote Control in the menu, instead of loading the Java applet, it will go straight to screenshot-based Remote Control instead. You can switch to Java based Remote Control from the toolbar, but you cannot switch back again. This setting is useful if you have an extremely slow connection or a browser without Java. For more information, see the appropriate part of this manual.

Audible Notifications

Beep when the remote control session starts or ends: If this is enabled the host computer will beep when a remote control session is initiated or ended.

Beep continuously during remote control: With this enabled the host computer will beep periodically when a remote control session is active.

Beep interval: Here you can specify the time between beeps for the above setting.

Interactive User's Permission

Ask for permission from interactive user: If you turn this option off, you will disable the icon, and also any attempts to notify the local user when someone is accessing the computer remotely. When this option is off, none of the other settings in this configuration screen apply. This option, when disabled, basically tells RemotelyAnywhere not to bother starting RAGui.exe, the software that sits in the system tray and communicates with the user. Disabling this option will also disable the Chat function.

Default answer for confirmation message: Yes or No. When someone tries to gain remote control access to the computer, and the local user does not answer the query, the remote control session will either proceed or not, depending on this setting.

Time allowed for the interactive user to give permission: This is the amount of time specified before the notification message times out.

Text to display to the user: This is the text that will be presented to the user in the remote control confirmation dialog box. The string '%USER%' will be substituted by the name of the user who is attempting the remote control operation.

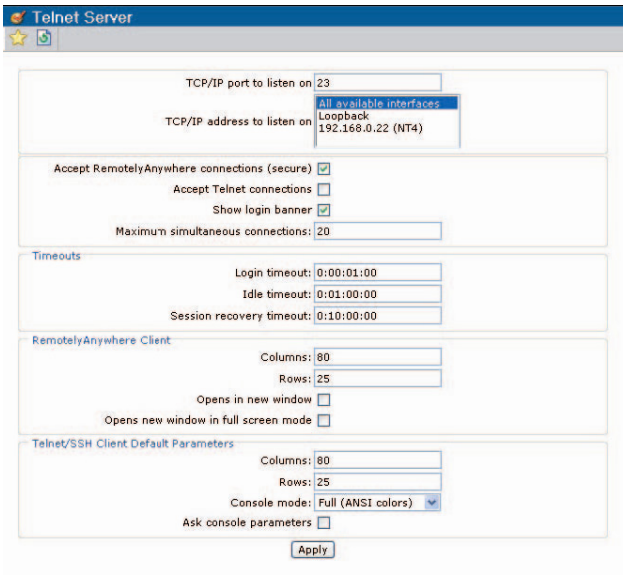
Display a warning message during Remote Control: Disabling this option requires a special license file.

Full Control (and Remote Control D) access rights bypass interactive user's permission: With this option enabled, users with full Remote Control access rights (R+W+D) will be able to access the remote host without first asking the user's permission. If this is enabled it overrides the above settings.

Remote Printing

Here you can enable or disable RemotelyAnywhere's ability to print remotely.

Telnet Server



This dialog box allows you to view and modify Telnet related options. For a complete explanation of the Telnet server, please see the Computer Management section of this manual.

TCP/IP port to listen on / address to listen on: Here you can specify which port / address you want RemotelyAnywhere to listen on for telnet connections. This defaults to the standard telnet port of 23, and all available interfaces. Changes take effect when the service is restarted.

Accept RemotelyAnywhere connections (secure): Allow connections from RemotelyAnywhere's built in Command Prompt.

Accept Telnet connections: Allow plaintext terminal emulator connections. If disabled, only the built-in Java client can be used to access Telnet. This does not affect the SSH server.

Show login banner: Enable or disable the logon message sent by the Telnet/SSH servers when a connection is established. The logon message looks like the following:

> Windows NT Server 4.0 (build 1381) Service Pack 6
> RemotelyAnywhere Telnet/SSH Server v3.5.268
> Copyright (C) 1998-2001 3am Laboratories PL. All Rights Reserved.

Login:

If you do not want to let anybody who connects to the Telnet/SSH ports know the version of the operating system and RemotelyAnywhere, disable this option.

Maximum simultaneous connections: Here you can specify the maximum number of connections to the Telnet/SSH servers. It's a good idea to set a reasonable limit, especially on computers connected to the Internet. Every new connection uses resources on the computer.

Timeouts

Here you can set the login timeout (number of seconds the user may remain idle during the login process), the idle timeout (number of seconds the user may remain idle during a Telnet/SSH session) and the session recovery timeout. When a Telnet connection is broken ungracefully (that is, the user does not type exit at the command prompt) it is possible to reconnect to the session and continue work where it was left off for a period of time. You can specify the amount of time for which you want the lost telnet session to remain available. Any and all running programs started by the user in the Telnet session will be available when the session is resumed.

RemotelyAnywhere Client

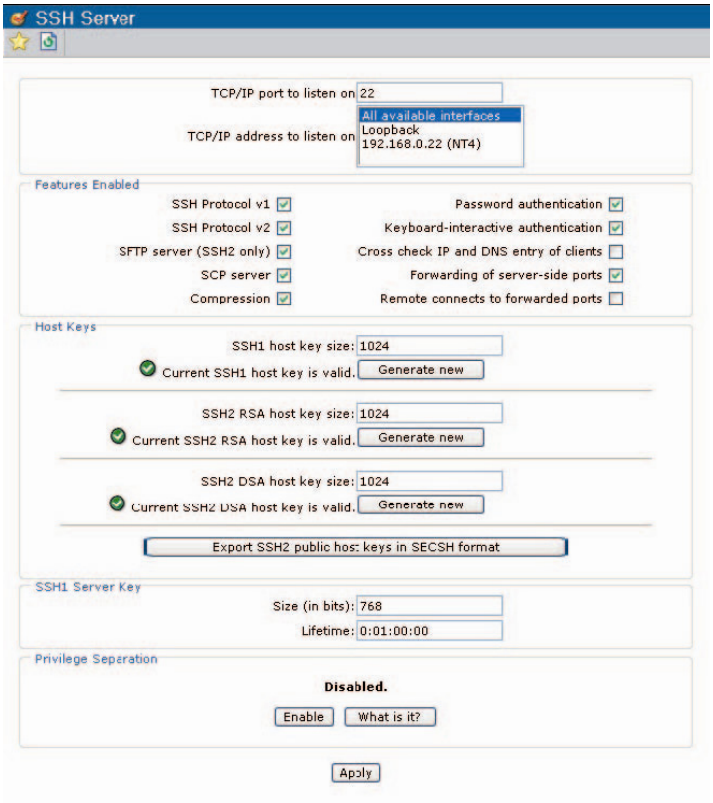
Here you can specify the number of columns and rows that the console window will occupy. You can also specify Whether You'd Like To Have The Client Open In A New Window, Or In A New Window In Full Screen Mode.

Telnet/SSH Client Default Parameters

Here you can specify the default parameters for the Telnet/SSH client. You can also select the console mode (Stream, Full ANSI Colors, or Full Monochrome) and enable/disable the console parameters option.

SSH Server

As with the Preference options for the Telnet Server, this dialog box allows you to view and modify SSH related options.



The IP and address options are the same as above, but with the default port of 22, which is standard for SSH connections. Changes will take effect when the service is restarted.

Features enabled: These are the nuts and bolts of the SSH server.

Enable SSH1 or SSH2: server to take advantage of these features.

SFTP: This is a secure file transfer method

SCP: This is another secure file transfer method, but non-interactive.

Compression: If this is checked data sent over the network will be compressed.

Password authentication: When activated, the user can enter a username / password combination in the terminal emulator client program and use that to gain access.

Keyboard interactive authentication: This is similar to the above option, but it won't allow the saving of the username / password in the terminal client.

Cross-check IP and DNS entry of clients: If this option is activated, and if the client comes from the IP address 192.168.0.10 (for example), and this IP address resolves to COMPUTER1, but COMPUTER1 does not resolve to 192.168.0.10, the connection will be disallowed.

Forwarding of server-side ports: This is SSH Port Forwarding, allowing server-side ports to be forwarded to others, effectively creating a virtual encrypted tunnel for the duration of the SSH session.

Remote connects to the forwarded ports: This allows the ports to be forwarded outside the server; that is, to any computer on the network the server has access to.

Host Keys

The SSH Host Keys section lets you re-generate SSH1 and SSH2 host keys used by the SSH server. You can specify the key size, but the larger the key, the longer it takes to generate it. Anything above 2048 bits is excessive, and will take a very long time even on a fast computer.

SSH hosts have keys that can be used to identify them, much like SSL-protected websites have certificates. SSH1 only supports a single host key, while SSH2 supports both RSA and DSA keys. The key length is recommended to be 1024 bits or more, and can be 512, 768, 1024, 2048 or 4096. The SSH1 server key is a key that is relatively short, and has a short lifetime. It is used in conjunction with the host key to negotiate a one-time session key for each connection. SSH2 uses the Diffie-Hellman keyexchange protocol to negotiate the session key and therefore does not need one.

Export SSH2 public host keys in SECSH format: This button lets you export the host keys and save them in your terminal emulator. This way, you can be sure that when the emulator connects to the RemotelyAnywhere computer and does not put up a warning about an unknown host key, you are still in fact connecting to the intended computer.

Privilege Separation

You can enable or disable privilege separation here. A full description of what this means is available within RemotelyAnywhere by clicking on 'What is it.' The text is reproduced here in full for your reference.

Privilege Separation In SSH

When a user establishes an SSH session, and authentication succeeds, the server executes applications (typically a shell process such as cmd.exe) in the user's security context. The server needs to execute with LocalSystem privileges to access resources required for user authentication and impersonation.

Allowing an anonymous user to directly communicate with code that runs with the same permissions as the

operating system itself is the primary reason remote exploits exist.

Privilege separation has been pioneered by the Unix community with the release of OpenSSH 3.2. The main goal of this technology is to prevent anonymous clients from exchanging information with highly privileged software. This is achieved by serving a client with the help of two server-side processes: one that runs with SYSTEM privileges, and another which has practically no privileges (i.e. GUEST privileges). The latter process is automatically spawned by the privileged parent. The unprivileged child processes all network data and handles communications with potentially untrusted clients. It relies on the parent process to perform tasks that need privileges, and communicates these requests through a well defined and very simple interface. This way both sides must agree that the client has authenticated before it is granted further access, and even if the unprivileged child is compromised, the intruder cannot gain access to, let alone modify, valuable information.

OpenSSH runs the unprivileged process in the context of a special user account. When you enable SSH Privilege Separation in RemotelyAnywhere, this user is automatically created and its access rights are minimized on the file system and the registry. This usually requires several minutes, especially on large file systems. This special user has very limited rights: only execute permissions in the System32 directory, and read rights to a minimum set of registry entries. These permissions are required by Windows to execute any and all software. All other access rights are explicitly denied for the special user account.

The Privilege Separation User is created under the name __ra_ssh_privsep__. It is maintained by RemotelyAnywhere and you should not modify the account, its group memberships or any other related security settings. This user is created with GUEST privileges, its password is set to a cryptographically random string that is as long as system policies allow. The user account is disabled by default. When RemotelyAnywhere accepts an SSH connection, it changes the user's password, enables the account, logs the user in, stores it's access token handle, resets the password again - and finally disables the user account until it is needed again.

Warning!

Only NTFS file systems allow the required access rights to be set.

When you install a new hard drive in your computer, Windows grants full access to the everyone group to the new hard disk and all of its contents. On such occasions you should use the Check rights feature on the SSH Configuration page to set the correct access permissions on your system.

Local or domain security policies might restrict local logins. RemotelyAnywhere attempts to explicitly grant the Privilege Separation User local login privileges in the local security policy - however, if domain policies override the local security policy, the __ra_ssh_privsep__ user might not be allowed to log in. In this case, Privilege Separation should be disabled or the domain security policy should be changed to be less restrictive.

Network Maintenance

With this feature you can install and configure RemotelyAnywhere on other computers connected to the network, much as you would with the RemotelyAnywhere Console.

This option will not work if you have logged on with NTLM authentication. NTLM authentication cannot be delegated over the network, so RemotelyAnywhere would not be able to identify you to other computers.

First, you are asked how you would like to scan the network. You can choose to scan a specified domain only, or you can browse the whole network. On larger networks, this can be a lengthy operation, so looking at single domains at a time is recommended. You also have the option of inspecting and upgrading a single computer.

On the next screen you are shown the part of the network selected in the previous step. All computers are listed, and you will be able to see what operating system and which version they are running, what roles they fulfill, and last, but not least, whether or not they have RemotelyAnywhere installed.

If RemotelyAnywhere is installed on a machine in the list, you can quickly open it by clicking on the machine name. You can also see which version of RemotelyAnywhere is running on the computer, and you can upgrade it if necessary with two mouse clicks.

If RemotelyAnywhere is not installed on one of the machines on the network you can also quickly do so from here with two clicks.

Command Line Parameters

In Windows NT and Windows 2000, you can run RemotelyAnywhere from the command line to perform various actions. These are:

Installing RemotelyAnywhere on the Local Computer

The command for this operation is:

Install [-port PORT]

You will need to have the RemotelyAnywhere installation files in the current directory, either copied from an existing installation or from the manual installation archive available on RemotelyAnywhere.com.

This command will create the RemotelyAnywhere service and its support driver in the current directory, and start it immediately.

The optional parameter can specify the listener port. For example:

RemotelyAnywhere Install -port 2020

You will need administrative privileges on the local computer to successfully perform this operation.

Installing Remotelyanywhere On A Remote Computer

The command is:

Install <–computer COMPUTER> <–path PATH> [-port PORT]
[-minimal] [-license FILENAME]

You will need to have the RemotelyAnywhere installation files in the current directory. You will also need administrative rights on the remote computer.

The first optional parameter is the same as when installing RemotelyAnywhere on the local computer; it specifies the HTTP port number. The [-minimal] switch allows you to perform a minimal install. This option does not copy the documentation files, thus speeding up the install process over a slow network connection. The two required parameters are the name of the remote computer and the local path to the intended destination directory on the remote computer.

The [-license FILENAME] option lets you specify a license file to be installed on the target computer.

For example, if you want to install RemotelyAnywhere on a computer called KOSSUTH in the C:\RemotelyAnywhere directory, and you do not want the documentation files copied, you will need to enter the following command:

RemotelyAnywhere Install –computer KOSSUTH -path "C:\RemotelyAnywhere" -minimal

This will create the destination directory, copy all necessary files, and create and start the RemotelyAnywhere service on KOSSUTH.

Uninstalling Remotelyanywhere On A Local Computer

The command is:

Uninstall

This will stop and remove the RemotelyAnywhere service and its support driver, as well as all registry entries created by RemotelyAnywhere. You will need to delete the RemotelyAnywhere directory and all its contents yourself.

For example:

RemotelyAnywhere Uninstall

You will need administrative privileges on the local computer to successfully perform this operation.

Uninstalling Remotelyanywhere On A Remote Computer

The command is:

Uninstall <-computer COMPUTER>

This will stop and remove the RemotelyAnywhere service and its support driver, as well as all registry entries created by RemotelyAnywhere. You will need to delete the RemotelyAnywhere directory and all its contents yourself.

For example:

RemotelyAnywhere Uninstall –computer KOSSUTH

You will need administrative privileges on the remote computer to successfully perform this operation.

Starting And Stopping A Service

The command is:

start [-service SERVICE] [-computer MACHINE]

stop [-service SERVICE] [-computer MACHINE]

The optional parameters are the name of the service (it defaults to RemotelyAnywhere) to be started, and the computer to perform the operation on (defaults to the local computer).

For example:

RemotelyAnywhere start

This will start the RemotelyAnywhere service on the local computer.

RemotelyAnywhere stop W3SVC –computer KOSSUTH

This will stop the W3SVC service on the computer called KOSSUTH. You will need administrative rights on the remote computer to perform this operation.

Restart The Remotelyanywhere Service

The command is:

Restart [-computer COMPUTER]

The optional parameter is a computer name (defaults to the local machine).

For example:

RemotelyAnywhere Restart –computer KOSSUTH

You will need administrative privileges on the computer to successfully perform this operation.

Export/Import RemotelyAnywhere Configuration Settings To/From A Text File

The commands are:

CreateIniFile [-inifile FILENAME] [-computer MACHINE]

LoadIniFile [-inifile FILENAME] [-computer MACHINE]

The default value for FILENAME is RemotelyAnywhere.ini in the directory the RemotelyAnywhere executable is located in. The COMPUTER parameter, if not specified, defaults to the local computer.

You can use these commands to quickly copy configuration settings from one RemotelyAnywhere installation to another, usually when installing RemotelyAnywhere to a remote computer from the command line.

A typical set of commands using these settings would be:

RemotelyAnywhere CreateIniFile

RemotelyAnywhere Install –computer SERVER1

RemotelyAnywhere Stop –computer SERVER1

RemotelyAnywhere LoadIniFile –computer SERVER1

RemotelyAnywhere Start –computer SERVER1

The first line saves the local RemotelyAnywhere configuration to the default file. The second command installs RemotelyAnywhere on the computer named SERVER1. The third command stops the RemotelyAnywhere service on SERVER1 – necessary, because the previous command already started RemotelyAnywhere. The fourth command will read all settings from the default .ini file, and configure RemotelyAnywhere on SERVER1 accordingly. Finally, the last command starts RemotelyAnywhere.

The CreateIniFile command will write all RemotelyAnywhere configuration data to the target text file. The LoadIniFile command will import all configuration data contained within the text file to the target computer. This means that all configuration data is copied, including permissions, FTP Server settings, the license key, etc. If you do not want to import specific configuration items, you will need to edit the generated .ini file and remove these entries. The format of the generated .ini file is as follows:

[MetaData]

Creator=RemotelyAnywhere

CreatorBuildNumber=268

SourceComputer=SERVER2

Value0000=UseGraphRed

Value0001=VisitLength

Values=2

[UseGraphRed]

Type=REG_DWORD

Data=0

[VisitLength]

Type=REG_DWORD

Data=600

The above example, of course, is just a small part of the actual file generated. If you do not wish to copy, for example, the VisitLength setting, simply remove the ValueXXXX=VisitLength line from the MetaData section.

PDA Access

RemotelyAnywhere supports access via wireless handheld devices connecting using the http protocol. Not all handheld PDAs are the same. While RemotelyAnywhere is designed to operate on the most popular PDA devices and browsers, some features may appear different from one handheld to the next, and indeed in some cases certain functions have been deactivated altogether due to the limitations of some devices. However, in the case of devices running Pocket PC 2000/2002, Microsoft Windows Mobile 2003 for Pocket PC, or Microsoft Windows Mobile 2003 Second Edition for Pocket PC, RemotelyAnywhere offers the ability to perform desktop remote control.

Logging in to RemotelyAnywhere via a PDA is very similar to logging in via a desktop's web browser. Simply ensure your PDA is connected to your LAN, or, if necessary, the internet, and enter the appropriate IP address or web address and click OK. Authentication with PDA browsers is exactly the same as with other browsers. Enter your Windows username and password and, if necessary, the domain name, click **OK**, and you will be brought to the main menu.

Security Precautions

With HTTP and the PDA's browser interface, making secure SSL connections is very similar to the process found on other browsers: simply create an SSL certificate, install the certificate in your browser, and use HTTPS as the protocol.

Main Menu

Depending on the browser, you will see a menu similar to this when logging in:

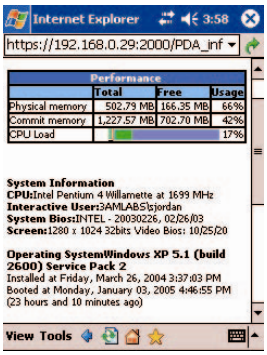
The clickable links are, in order:

- Home
- Remote Control
- Processes
- Services
- Drivers
- Event Viewer
- User Manager
- Registry Editor
- Reboot
- CPU Load
- Memory Load
- File Transfer
- Network Maintenance
- Log Out

The left-pointing arrow encased in the blue circle, present at the top of every page displayed by RemotelyAnywhere, provides a link back to this main menu.

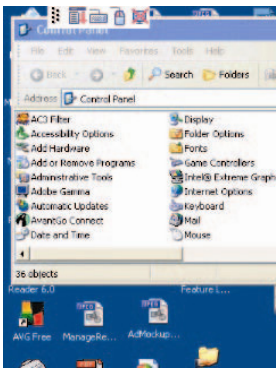
Home

A simplified version of the RemotelyAnywhere home page described earlier in this manual; the PDA interface's home page shows a simple system overview.

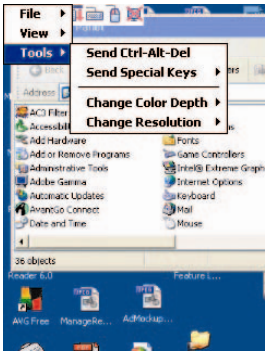


Remote Control

If this option is available with your browser, selecting **Remote Control** downloads an ActiveX control to your PDA.



Using the stylus, you can move the mouse around on the screen. Tapping the screen, as per normal, is like clicking the mouse.



The toolbar, seen at the top left, offers the following buttons in order from left to right:

Drag: Using this button, the toolbar can be dragged around the edges of the PDA window.

Menu The menu offers the following options:

File > Disconnect: Ends the RemotelyAnywhere session

View > Actual Size: Views the host screen at 100% magnification

View > Scale to Fit: Scales the host screen to fit the PDA screen

View > Zoom To >: Manually specify the zoom level

View > No Rotation: Maintains the remote control screen vertically represented

View > Rotate Left 90 Degrees: Rotates the remote control screen to the left

View > Rotate Right 90 Degrees: Rotates the remote control screen to the right

(The above two options make better use of the screen geometry of the PDA, thus allowing a larger picture)

Tools > Send Ctrl-Alt-Del: Sends a Ctrl-Alt-Delete keystroke combination

Tools > Send Special Keys: See Remote Control section of this manual

Tools > Change Color Depth: Changes the number of colors shown on the host screen

Tools > Change Resolution: Changes the screen resolution of the host screen

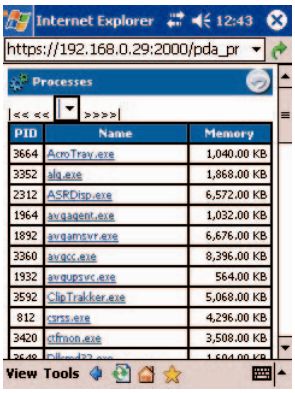
Keyboard: Tapping this icon once brings the keyboard interface up, allowing you to type. Tapping it again makes the keyboard disappear.

Mouse button: Tapping this icon switches between left and right mouse-clicks.

Exit: Returns to main menu.

Processes

The Processes page has three options, as shown:

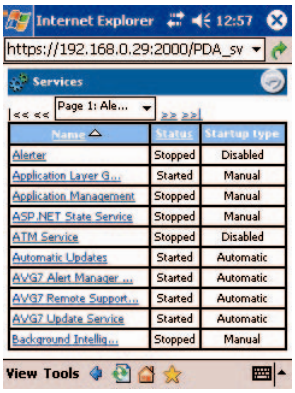


The output of this function will give you a listing of all processes running on the remote computer. The list is hierarchical: a parent process will have its child processes listed beneath it, with indentation indicating relationships. Please note that this is for information purposes only, since Windows reuses process IDs.

Selecting a process will give you more information about it, as detailed earlier in this manual.

Services & Drivers

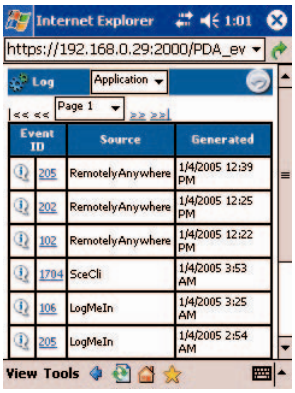
The image below shows you what you would see under the services or drivers menu options:



The format of the Services and the Drivers lists are identical. These lists display the names and statuses of all the services (or drivers) installed on the remote machine. Clicking on the name will show you more detail about the selected object and allows you to control it. You can also change its startup options. When specifying a user account to be used by a service, it must be in DOMAIN\USER form. If you want to use a local user account, you can type .\USER.

In the list of objects, the status field shows Stopped, Running, Starting, Stopping, etc. RemotelyAnywhere looks through the list of services and drivers, and if it finds one that is set to start automatically but is not running, a question mark is displayed. This alerts you to the fact that the service should be running, but isn't.

Event Viewer

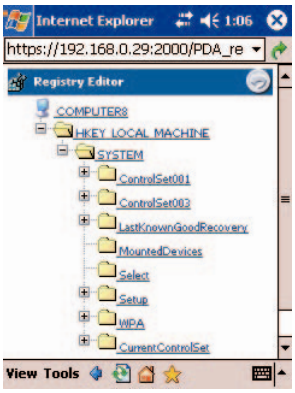


This option enables you to view RemotelyAnywhere's event viewer. You will be given a list of event viewer options as in the image on the left.

User Manager

When you click on User Manager in the menu you will be able to access RemotelyAnywhere's use manager. Supporting all the features of NT's built-in User Manager, its functionality is similar to that of RemotelyAnywhere's regular User Manager.

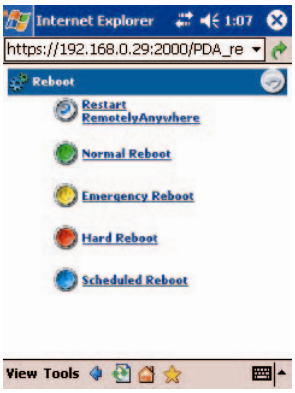
Registry Editor



This option enables you to edit the registry of the host computer. First, the registry roots (HKCR, HKCU, HKLM, etc.) are displayed, and you can drill down into them by clicking on their names. Registry keys are links that open up that key for you. Key values are also displayed here, with their name, type and value. You can edit values that are of either text (REG_SZ, REG_EXPAND_SZ or REG_MULTI_SZ) or integer (REG_DWORD) type. Binary, etc. values are only displayed but cannot be edited. Using the buttons at the bottom of every page you can add a subkey, add a value or delete the currently opened key.

Reboot

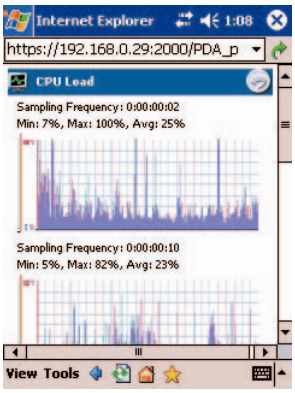
This option presents you with a menu similar to that found in the HTML interface.



The first selection restarts the RemotelyAnywhere service.

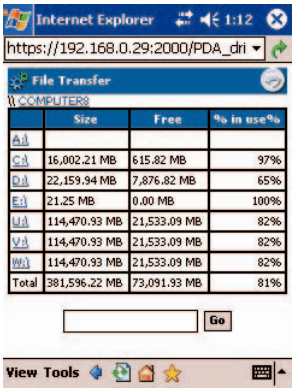
The next four selections reboot the computer. Normal reboot shuts down all applications. Emergency reboot kills all processes then shuts down and restarts the system in an orderly fashion. You might lose data in your running applications. Hard reboot is just like pressing the reset button or toggling the power switch: use this only as a last resort! Scheduled reboot allows you to reboot the remote machine at a specified time.

CPU Load & Memory Load



Here you can view graphs on the CPU and memory load.

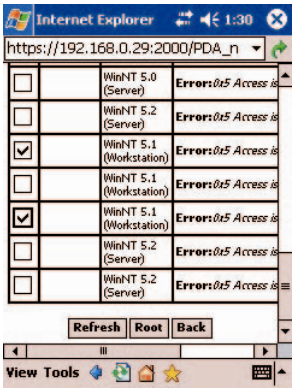
File Transfer



When using File Transfer, bear in mind that Palm devices do not really have a "traditional" file system. Under the Windows CE browser, you can hover your stylus over a file and it will give you the option to "Save as" (thus putting the "transfer" in "file transfer") whereas on the Palm OS, all it will do is try to open files in various programs (for example, text files in textpad and jpgs in a picture viewer).

This is the fundamental difference between Palm and Windows CE.

Network Maintenance



With this feature you can install and configure RemotelyAnywhere on other computers connected to the network, much as you would with the RemotelyAnywhere Console, as documented in the Preferences chapter of this manual.

Log Out

This menu option ends your RemotelyAnywhere session.

It is not strictly necessary to manually log out – your session will eventually time out after the time period specified in the RemotelyAnywhere configuration elapses.